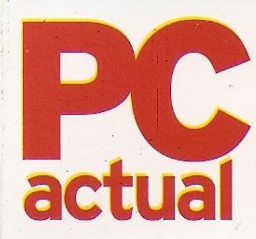
Suplemento PC Actual nº 218 + DVD 51

LOS MEJORES TRUCOS Y CONSEJOS



Guía Práctica

by CosmosXXI

Tu PC más seguro



> **Haz de tu equipo una fortaleza**
- Backups
- UAC en Vista
- Actualizaciones

> **Encriptación**
- Sistema EFS
- BitLocker
- Fotos y vídeos
- Codificación PGP

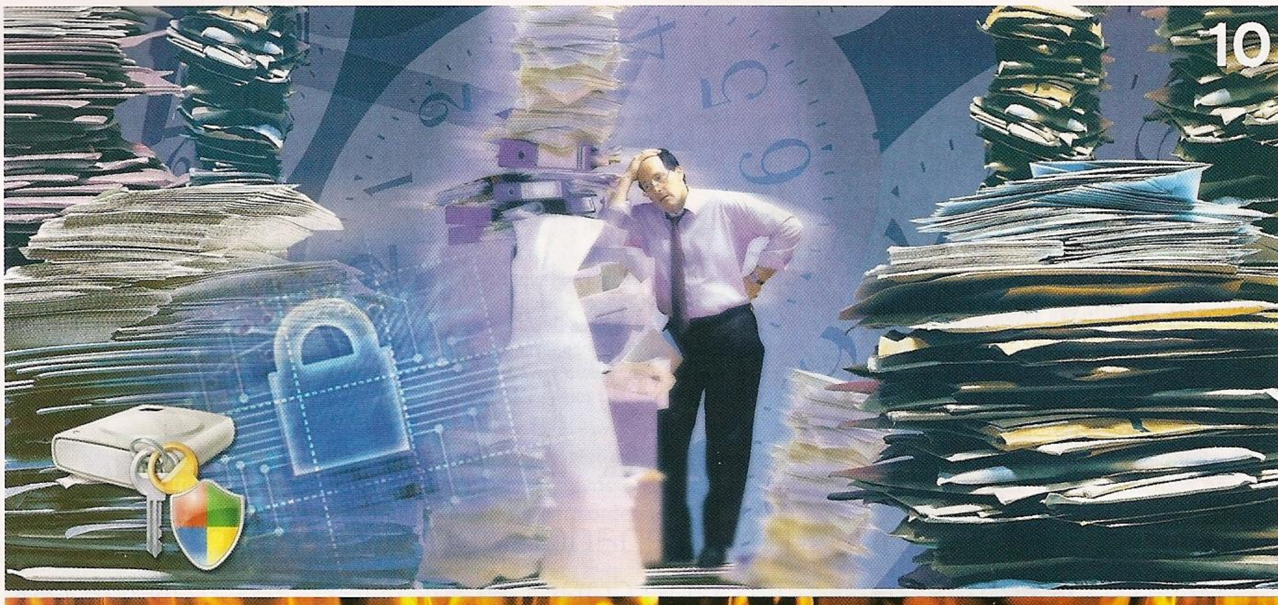
> **Red local e Internet**
- Firewall de Windows
- ZoneAlarm
- Router ADSL
- Navegadores
- Conexión WiFi

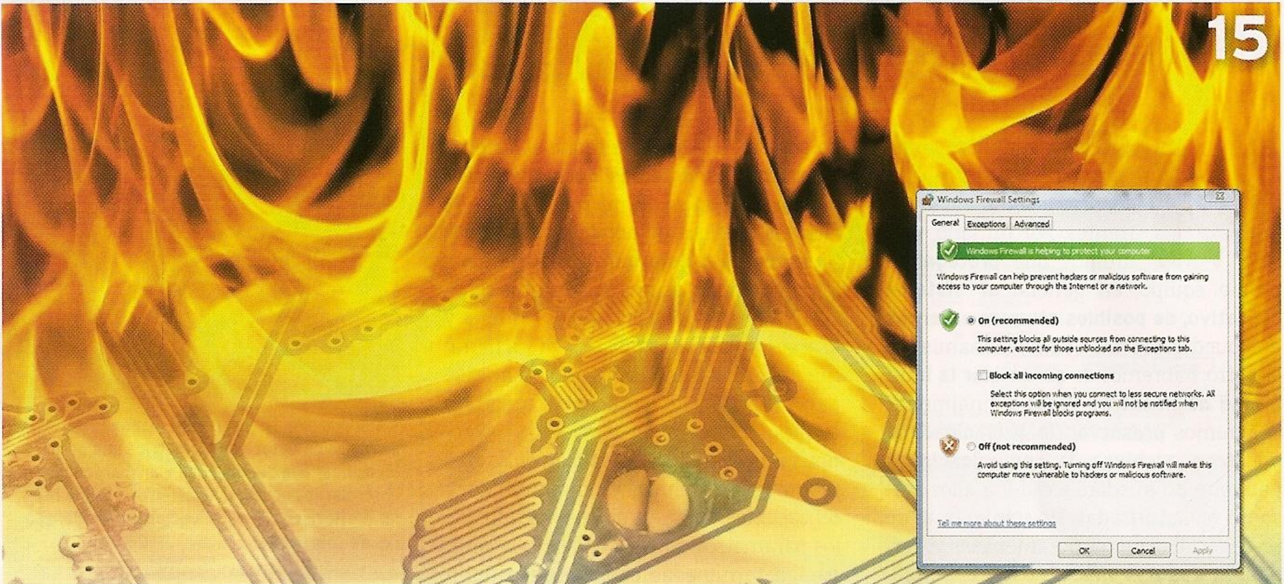
> **Herramientas**
- Antivirus
- Antispyware
- Rootkits

> **Comprobaciones**
- Servicios de diagnóstico
- Botnets y zombies

> **Privacidad**
- Navegación
- Correo electrónico
- Dirección IP
- Contraseñas

Tu PC más seguro





PROTEGE TUS DATOS Y TU SISTEMA DE CUALQUIER TIPO DE AMENAZA

HAZ DE TU PC UNA FORTALEZA

Para salvaguardar nuestro ordenador y preservar la privacidad de nuestros datos, tenemos que conocer primero las amenazas a las que estamos expuestos los usuarios.

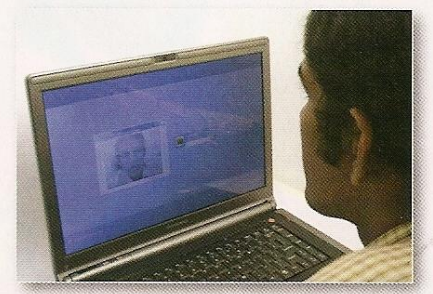
Mantener seguro un ordenador es una tarea que se proyecta en distintos frentes. Por un lado, tendremos que **proteger** al propio equipo, en general **al sistema operativo, de posibles ataques externos** que puedan afectar a su funcionamiento. Por otro, habremos de **garantizar la integridad de nuestros datos** y, finalmente, deberemos **preservar la privacidad de nuestros archivos y comunicaciones** para que no puedan acceder a ellos personas no autorizadas. No solo se trata de proteger al sistema de amenazas externas, programas maliciosos, vulnerabilidades o *hackers*, sino también de descuidos que pueden exponer nuestros datos o archivos privados tanto a su destrucción como a los ojos indiscretos de terceros. Una *password* demasiado obvia o simplemente dejar el ordenador encendido sin activar un salvapantallas con contraseña pueden acabar con las precauciones de seguridad más estrictas.

Control de acceso

Uno de las barreras básicas para conseguir que un sistema sea seguro es la del control de acceso, el **asegurarse de que quien accede al ordenador queda perfectamente identificado** y se le otorga control y acceso a los datos y recursos que le han sido asignados. El **control** de acceso más severo es el **físico**, el que no permite a un usuario utilizar el sistema si no demuestra su identidad. Existen múltiples sistemas hardware que permiten realizar comprobaciones de identidad, como el que utilizan sistemas biométricos (normalmente la huella dactilar) o una tarjeta identificadora. La siguiente barrera de acceso es la que interpone el sistema operativo. Los **sistemas operativos modernos** disponen de un mecanismo de cuentas en el que **un administrador asigna recursos a determinados usuarios** a los que también asigna una palabra clave. Como veremos, el restringir los recursos y el acceso a los datos puede ser una herramienta de seguridad eficaz no solamente para sistemas a los que acceden múltiples usuarios, sino también para entornos monousuario. Limitar la ejecución de ciertos programas o archivos y no permitir modificaciones del sistema son algunos de los parámetros que se pueden establecer para determinadas cuentas de usuario. La gestión de cuentas debe ser la primera herramienta de seguridad para proteger nuestro ordenador y sus datos, sobre todo si compartimos su uso.

Amenazas exteriores

En la actualidad, es bien sabido que la mayor parte de las amenazas para ordenadores domésticos provienen del exterior. Existen **programas** clasificados como *malware* que utilizan distintos métodos de intrusión dentro de nuestro ordenador **para acceder a nuestro sistema**, ya sea **para obtener información** sin nuestro consentimiento **o** para **deteriorar** el sistema o los datos que contiene. También existen **programas que permiten al que los distribuye tomar control de nuestro ordenador o de parte de sus recursos** sin que nosotros lo sepamos. Este *malware* tiene distintas formas para extenderse, desde la explotación de vulnerabilidades del sistema operativo, del navegador y otro software (como complementos multimedia) hasta el uso de la ingeniería social. La prudencia y el sentido común suelen ser útiles para prevenir problemas con este tipo de programas dañinos, así como



• **Algunos equipos portátiles disponen de sistemas de detección biométrica que permite identificar a la persona que usa el ordenador y controlar los accesos. También es posible instalar periféricos con esta función para ordenadores de sobremesa.**

Warning - visiting this web site may harm your computer!

Suggestions:

- Return to the previous page and pick another result.
- Try another search to find what you're looking for.

Or you can see the image in its own context http://www.phonarcom.com.ar/5d_pdf/WRT-415.htm at your own risk. For detailed information about the problems we found, visit Google's Safe Browsing diagnostic page for this site.

For more information about how to protect yourself from harmful software online, you can visit StopBadware.org.

If you are the owner of this web site, you can request a review of your site using Google's Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

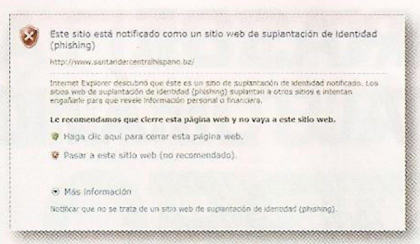
Advisory provided by Google

• **Además de los navegadores y otras aplicaciones, algunos buscadores de Internet también disponen de sistemas de detección de acceso a páginas web potencialmente peligrosas.**

disponer de herramientas de prevención actualizadas y eficaces, como veremos en el capítulo correspondiente. En ocasiones, las amenazas exteriores están más cerca de lo que creemos. Es el caso de los **hackers** que logran introducirse en las redes *wireless* y consiguen **acceso a nuestra red local**. Las comunicaciones son otra parte vulnerable a la hora de dibujar nuestro mapa de seguridad y herramientas como los *firewall* pueden ser muy eficaces para atajar posibles problemas como intentos de controlar nuestro PC o fugas de datos.

Privacidad

Además de mantener nuestros datos y sistema a salvo de problemas, también nos aseguraremos de que nadie pueda obtener archivos o datos confidenciales desde nuestro ordenador. En este sentido, junto a la prevención ante accesos no autorizados a nuestros ficheros, a veces, es conveniente utilizar herramientas para **cifrar los archivos**, de forma que solo los puedan utilizar aquellas personas a los que van destinados. En Internet, el cifrado se emplea para los datos más sensibles, como las transacciones con tarjetas de crédito o con la Administración. Nosotros podemos recurrir a él para proteger unidades de disco o mensajes de correo electrónico. Al igual que la protección de amenazas exteriores, la privacidad también pasa por el sentido común. No olvidemos que prácticas como el *phishing* pueden conseguir que proporcionemos nosotros mismos nuestros datos personales. ■

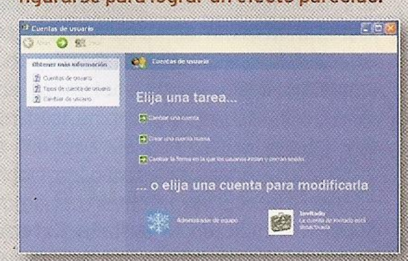


• **Los ataques de ingeniería social como el phishing aprovechan el descuido de los usuarios. Para evitarlos, además del sentido común, algunos navegadores utilizan bases de datos con sitios web sospechosos para advertir de su peligrosidad si los visitamos.**

EL DECÁLOGO DE LA SEGURIDAD

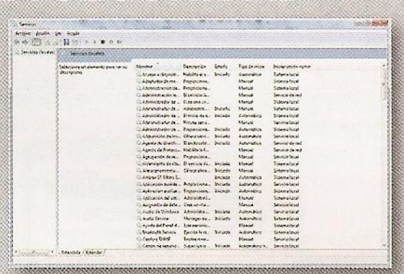
En los capítulos que mostraremos a continuación, veremos explicaciones prácticas de cómo aumentar la seguridad de nuestro ordenador utilizando distintas herramientas. Sin embargo, en muchas ocasiones, unos buenos y sencillos consejos pueden aumentar significativamente el nivel de fiabilidad. Vamos a ver diez de las sugerencias más importantes para que nuestro ordenador esté más seguro.

1) No utilizar la cuenta de administrador para navegar. Lo más indicado es crear una cuenta sin privilegios de administrador. Es un consejo importantísimo que no se suele seguir por la comodidad de tener permisos para instalar software. Sin embargo, el *malware* también encontrará esa facilidad. Como veremos, el UAC puede configurarse para lograr un efecto parecido.



2) Actualizar. Una de las principales fuentes de problemas de *malware* es no actualizar el sistema operativo y aplicaciones como el navegador. Windows provee de lo necesario para actualizarlo en todo momento y algunas aplicaciones, como navegadores y antivirus, también pueden hacerlo de forma automática.

3) Conocer qué servicios están activos en el sistema. Es una excelente política saber qué servicios se encuentran activos en el sistema y eliminar aquellos que no precisemos. Es habitual que servicios como FTP o Telnet estén habilitados y, sin embargo, no son necesarios. Mejor desactivar cualquier servicio del sistema que acceda a Internet y que no usemos.



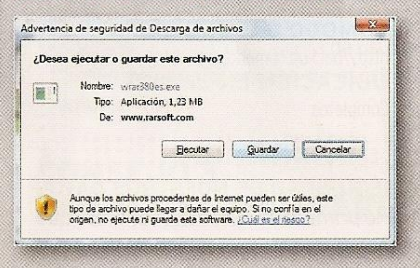
4) Defender el perímetro. La llamada defensa de perímetro en informática es la que constituyen los *routers* o *firewalls* hardware. Es una defensa externa al ordenador que se muestra muy eficaz. En ocasiones, será bueno adquirir un *router* más completo que el proporcionado por nuestro proveedor ADSL y que disponga por lo menos de sistema de protección NAT.

5) Copias de seguridad periódicas. Otro engorro impopular pero que puede salvar muchos datos importantes. Veremos cómo programar copias de seguridad de forma que el engorro sea lo menor posible, además de establecer puntos de restauración del sistema antes de instalar cualquier programa (una costumbre muy saludable).



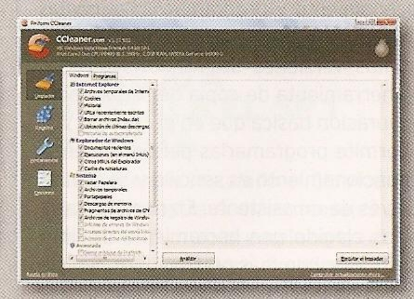
6) No confiar en redes extrañas. Con el auge de las redes wireless y los portátiles, es habitual utilizar redes inalámbricas para la conexión a Internet que no son las que conocemos. Siempre que nos conectemos a este tipo de redes, aunque sean de pago, tendremos que extremar las precauciones. Veremos en un artículo práctico cómo ocultar nuestras comunicaciones en este tipo de casos.

7) No ejecutar, guardar. Una buena práctica al descargar programas o instaladores es la de nunca aceptar la opción ejecutar al realizar la descarga. Lo primero, guardaremos el ejecutable en el disco, utilizaremos el antivirus y, luego, lo ejecutaremos de la forma más controlada posible.



8) Seguridad en la red local. Jamás se debe permitir acceso libre a los recursos de red, aunque se trate de una red doméstica. Siempre asignaremos palabras clave a cualquier carpeta compartida.

9) Atento a los síntomas. Cuando el sistema se comporte de una forma errática, es bueno realizar un chequeo completo con un antivirus y un limpiador de registros y del sistema en general.



10) Encriptar. La encriptación es más importante de lo que parece, sobre todo con ordenadores portátiles, pero, en general, en cualquier sistema. Por norma, hay que encriptar cualquier comunicación con datos personales y cualquier carpeta que contenga ficheros confidenciales.

REALIZA COPIAS DE SEGURIDAD AUTOMÁTICAS

SIEMPRE RESPALDADOS

Para conseguir que nuestro sistema sea más seguro, lo más importante es poner a salvo nuestros datos antes de que algún problema pueda ponerlos en peligro.



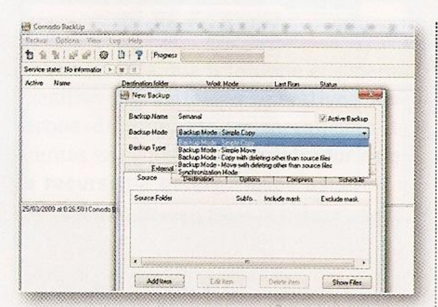
INCLUIDO EN EL DVD

COMODO BACKUP
http://backup.comodo.com
UBICACIÓN EN EL DVD
Completos

LA SEGURIDAD DE NUESTROS DATOS es de lo primero de lo que nos tenemos que preocupar, no solo protegiéndolos de amenazas externas, sino previniendo posibles problemas, de forma que estén siempre a buen recaudo. Realizar copias de seguridad periódicas hará que nuestros datos estén a salvo independientemente de las amenazas, errores e incluso descuidos por nuestra parte. Las aplicaciones de *backup* permiten utilizar distintos sistemas de almacenamiento y programar estas copias para que se realicen automáticamente. Las distintas versiones de Windows ofrecen una herramienta de copia de seguridad y restauración básica que en el caso de Vista permite programarlas periódicamente. Su funcionamiento es sencillo y se realiza a través de un asistente. En nuestro caso, hemos elegido una herramienta de libre distribución con más prestaciones. Se trata de la aplicación **Comodo BackUp**, que podemos descargar desde **http://backup.comodo.com** o instalarla directamente desde el DVD.

PASO 1
»NUEVO PROCESO DE BACKUP

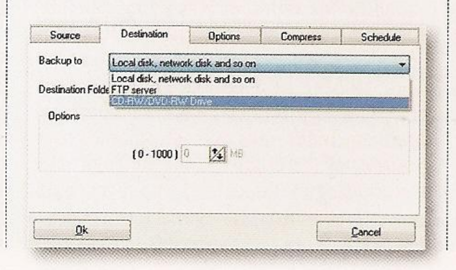
El primer paso es crear un nuevo proceso de backup con **Comodo**. Para ello, haremos clic en la parte superior izquierda,



en el icono con el símbolo **+**. En la ventana que aparece, completaremos la información que se nos solicita. En primer lugar, escribiremos el nombre del proceso. Luego, elegiremos entre copia simple, mover (borrando los archivos originales), copia de seguridad y borrado de los archivos antiguos en el sistema de almacenamiento, o mover los datos borrando tanto los archivos originales como los antiguos en el sistema de almacenamiento. El **Sinchronization mode** realiza copias de ficheros según se van creando.

PASO 2
»DEFINE LOS DATOS

En la pestaña **Source** pulsaremos sobre el botón **Add Item** y elegiremos carpetas, **Mis Documentos** o el buzón de entrada de **Outlook** para realizar la copia. En **Destination** podemos elegir el sistema de copia que vamos a utilizar, incluyendo unidades de discos locales, en red, servidor FTP o



grabadora. Para que la copia ocupe menos espacio, pulsaremos en la pestaña **Compress** para crear archivos ZIP. Incluso podemos agregar la fecha y hora de la copia al nombre del fichero comprimido.

PASO 3
»PROGRAMA COPIAS

Abriremos la pestaña **Schedule** para decidir si queremos programar las copias por días o por meses. Luego, definiremos la hora a la que se realizarán. También podremos concretar si queremos que la copia se ponga en marcha al abrir, al cerrar la aplicación o cada cierto número de horas. Al pulsar en **OK**, se almacenará el proceso de copia, que se pondrá en marcha en el momento elegido.

PASO 4
»OTROS DETALLES

Si hacemos clic en la pestaña **External Task**, podremos programar que se ejecute alguna aplicación antes o después de poner en marcha la copia de seguridad programada. Desde **E-mail notify**, será factible introducir los datos de una cuenta de correo (que podemos crear especialmente para el *backup*) que nos notificará si se ha realizado la copia sin necesidad de estar presentes. Bajo **Test**, ejecutaremos una prueba de la copia para comprobar si hemos elegido los parámetros correctos. Finalmente, para la **recuperación de la copia de seguridad**, acudiremos a la ventana principal del programa y haremos clic en la opción **Backup** del menú. A continuación, elegiremos **restore from local machine**. Luego, seguiremos los pasos indicados por el programa pulsando **Next** a cada momento. ■

AUMENTA LA FIABILIDAD CON ESTA FUNCIÓN DEL SISTEMA

SÉ TÚ QUIEN DOMINE EL UAC

Una de las funciones más denostadas de Vista es el UAC, el control de acceso de usuario, que puede resultar molesta pero que aumenta la seguridad.

LA FILOSOFÍA DEL UAC (*User Access Control* o **Control de Acceso de Usuario**) es sencilla, se trata de una herramienta que permite **comprobar** si el que está realizando un **cambio en el sistema**, como la instalación de un ejecutable, o **modificaciones en su configuración** es un usuario o una aplicación. Por otro lado, comprueba que el usuario tiene privilegios suficientes para realizar esta acción.

Siempre que detecta una de estas alteraciones, el UAC muestra una ventana de diálogo que pide confirmación manual de las acciones que se van a realizar. Esto permite atajar de raíz los problemas que puedan producirse por *malware* que intente actuar sobre el sistema sin que lo sepamos. Sin embargo, también ha provocado cierto fastidio por parte de los usuarios, sobre todo aquellos acostumbrados a instalar un gran número de aplicaciones en Windows XP. Y, la verdad, resulta algo engorroso, pero es necesario para nuestra protección. Vamos a ver una serie de consejos y pequeños trucos para conseguir que el UAC nos proteja al máximo y sea menos molesta.

CONSEJO 1 »DESACTIVA LA UAC DE FORMA TEMPORAL

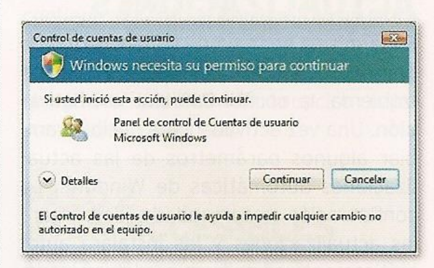
Aunque han aparecido trucos que permiten desactivar el sistema UAC editando ciertas entradas de Registro, no es recomendable desactivarlo permanentemente.



Si queremos hacerlo de forma temporal, porque, por ejemplo, tenemos que realizar un gran número de instalaciones, acudiremos al **Panel de control/Cuentas de usuario/Protección infantil** y, finalmente, a **Cuentas de usuario**. Luego, haremos clic sobre **Activar o desactivar el Control de cuentas de usuario**.

CONSEJO 2 »AVISOS

Los avisos del UAC se presentan en ventanas que muestran distintos colores, según la importancia de los cambios que se pretenden hacer. Debemos estar atentos sobre todo a los más importantes. Los mensajes del UAC aparecerán en las siguientes situaciones:



- Instalación o desinstalación de software.
- Instalación de un controlador.
- Uso de la consola de **Windows Update** para instalar las actualizaciones.
- Exploración del directorio de otro usuario.
- Configuración del control parental.
- Instalación de un control ActiveX.
- Al abrir o cambiar la configuración de control del *firewall* de Windows.
- Cambios del tipo de cuenta de usuario.
- Modificación de la configuración de seguridad con el complemento **Editor de directivas de seguridad (secpol.msc)**.
- Configuración de las actualizaciones automáticas.
- Restauración de archivos de sistema de los que hay una copia de seguridad.
- Programación automática las tareas.
- Al copiar o mover archivos en el directorio archivos de programa o el directorio de Windows.
- Al agregar o quitar una cuenta de usuario.
- Configuración del acceso de escritorio remoto.

CONSEJO 3 »DETECTA MALWARE

La aparición de un **aviso de UAC** nos permite saber si un programa está intentando modificar partes del sistema sin que lo sepamos. Si vemos que aparece un aviso del UAC sin que hayamos realizado ninguna de las tareas detalladas en el segundo punto, es probable que suframos el ataque de un *malware*, por lo que realizaremos un **chequeo del sistema** en busca de ellos.

CONSEJO 4 »INSTALA EL SP 1 DE VISTA

Si no tenemos instalado el Service Pack 1, el UAC mostrará más mensajes de lo necesario. Con solo emplazarlo, el UAC será menos fastidioso. En Windows 7, los mensajes del UAC han sido reducidos aún más. Podemos comprobar si tenemos instalado el Service Pack 1 abriendo el **Panel de control/Sistema y mantenimiento** y, finalmente, **Sistema**. Si el sistema no dispone de esta actualización, acudiremos a la página web **www.microsoft.es/descargas**. En **Familia de productos**, haremos clic en **Windows** y, a continuación, localizaremos el enlace correspondiente al **Service Pack 1** para proceder a su descarga e instalación. ■

PROCURA ESTAR AL DÍA
ACTUALÍZATE

El malware está en continua evolución para encontrar fallos en los sistemas operativos y programas. Por suerte, podemos evitarlo actualizándolos constantemente.

INCLUIDO EN EL DVD



APPSNAP
Comprueba si hay actualizaciones para el software de nuestro PC y las instala automáticamente
Contacto: Ganesh Viswanathan. http://appsnap.genotrance.com

RADARSYNC
Comprueba la actualización de controladores y software asociado
Contacto: RadarSync. www.radarsync.com

UBICACIÓN EN EL DVD
Completos

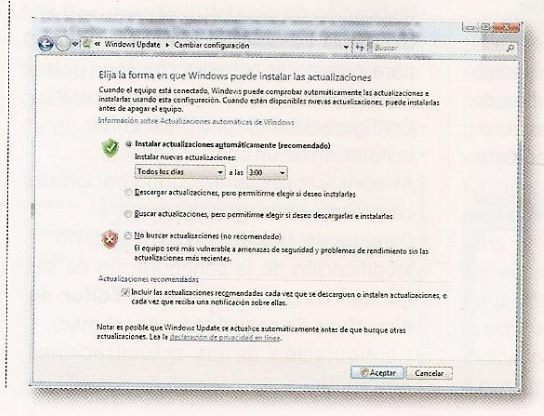
PONER AL DÍA EL SISTEMA operativo y las aplicaciones que tenemos instaladas en el ordenador, especialmente los navegadores de Internet y sus complementos, no solo es una práctica recomendable para **obtener el máximo de prestaciones** y nuevas funcionalidades, sino también permite **prevenir problemas de seguridad**. Los desarrolladores de *malware* y los *hackers* están en continua búsqueda de puntos débiles y fallos de sistemas operativos y programas para acceder a los recursos de nuestro ordenador. Cuando los fabricantes del software atacado reciben noticias de estas vulnerabilidades, suelen ofrecer actualizaciones para corregirlas. El **elemento más sensible es el sistema operativo**, que es el que da acceso a los recursos, pero los **navegadores** y sus complementos también son importantes, ya que constituyen la puerta de entrada. Cualquier otro software de nuestro ordenador, incluso los propios antivirus y otras herramientas de seguridad, también son vulnerables al aprovechamiento de fallos, por lo que su actualización es importante. Dado el peligro potencial y la frecuencia con la que aparecen vulnerabilidades, Windows dispone de un sistema de actualización automática llamado **Windows Update**, gracias al cual no tendremos que acudir a una página web para descargar los parches correspondientes. Además, en caso de que Microsoft considere que existe una actualización crítica urgente, Windows Update se encargará de instalarla. También algunos navegadores disponen de actualizaciones automáticas. En este práctico, veremos cómo configurar esta herramienta para que no tengamos que preocuparnos de que nuestro sistema operativo y aplicaciones estén al día.

PASO 1 »ACTIVA WINDOWS UPDATE EN VISTA

En primer lugar, vamos a configurar Windows Update en Vista para definir cómo se realizarán las actualizaciones automáticas. Para acceder a la configuración, haremos clic en el botón **Inicio**, luego, en **Programas** y pulsaremos sobre **Windows Update**. En la ventana que aparecerá, pincharemos en **Activar ahora**.

PASO 2 »CONFIGURA LAS ACTUALIZACIONES

En la misma ventana de Windows Update podremos encontrar, dentro de la columna izquierda, la opción **Cambiar configuración**. Una vez activada, será posible cambiar algunos parámetros de las actualizaciones automáticas de Windows. La configuración recomendada descargará las actualizaciones y las instalará automáticamente a una hora predeterminada. Podremos variar la hora de la actualización y adaptarla a nuestro ritmo de uso. Igualmente, tendremos la oportunidad de elegir una actualización semanal en vez de diaria. Como se advierte en esta ventana, en ocasiones Windows Update se actualizará antes de descargar los ficheros de actualización.



PASO 3 »ACTUALIZACIÓN MANUAL

En la misma ventana de Windows Update, podemos realizar actualizaciones manuales. Para ponerlas en marcha, haremos clic en la parte izquierda de la caja, en el enlace **Buscar actualizaciones**. Una vez localizadas las disponibles, se mostrará el número de actualizaciones aprovechables y el espacio que van a ocupar. Luego, pincharemos en **Ver actualizaciones disponibles**. Veremos en pantalla aquellas que se pueden instalar y se mostrarán cuáles son las importantes, recomendadas u opcionales. Las actualizaciones que queramos emplazar se seleccionarán marcándolas y pulsando en **Instalar**. Es posible pinchar con el botón derecho del ratón sobre las actualizaciones opcionales y elegir **Ocultar actualización** para que no se muestren la próxima vez en la lista.

PASO 4 »OTROS PRODUCTOS MICROSOFT

Si disponemos de otros productos de Microsoft, podremos programar su actualización de igual forma que lo hacemos con Windows. Para ello, en la ventana de **Windows Update**, haremos clic en **Obtener actualizaciones para más productos**. Ello abrirá una sesión de Internet Explorer que nos permitirá descargar e instalar **Microsoft Update** y que actualizará los productos de Microsoft al igual que se hace para Windows a través de Windows Update. ■

UN INSTRUMENTO DE DEFENSA MÁS
LA OCULTACIÓN DE LOS DATOS

La protección, además de defenderse de posibles amenazas externas, consiste también en poner a buen recaudo nuestra información encriptando nuestras carpetas y mensajes.

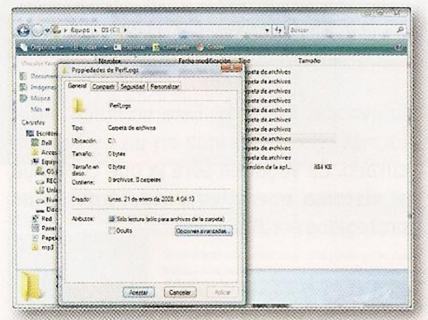
LA ENCRIPTACIÓN PUEDE suponer una segunda e importante barrera para proteger nuestros datos, sobre todo los confidenciales. De esta forma, aunque alguien consiga acceder a nuestro ordenador de alguna forma o intercepte nuestros mensajes de correo electrónico, no podrán descifrar el contenido de nuestros archivos o correos. La **encriptación utiliza técnicas de criptografía para transformar los datos en archivos indescifrables** a menos que dispongamos de la clave adecuada.

Esta estrategia de cifrado de ficheros puede ser conveniente si compartimos el ordenador o si utilizamos un PC portátil que puede quedar desatendido. Cualquiera puede acercarse a un ordenador con una memoria Flash USB y copiar datos confidenciales sin apenas esfuerzo. Si solemos llevar nuestros datos precisamente en llaves USB u otro tipo de sistemas de almacenamiento portátil, también es importante proteger los archivos que contienen con encriptación. De esta manera, si los extraviamos, no estaremos expuestos a que cualquier desaprensivo acceda a nuestra documentación.

Windows dispone de dos sistemas para encriptar: el **EFS** y la herramienta **BitLocker**. El primero se trata de un sistema básico de protección que puede utilizarse en **Windows Vista Business**, **Enterprise**, **Ultimate** y **XP Pro**. El resto de versiones de Vista solamente son capaces de descifrar carpetas EFS, pero no permite cifrarlas. Por otro lado, este método únicamente es compatible con el sistema de ficheros NTFS. Veamos un poco más sobre él.

PASO 1
»ENCRIPTA LA CARPETA EFS

Para cifrar los datos de una carpeta con EFS, tendremos que abrir el Explorador de Windows y localizar aquella que queremos encriptar. Enseguida, haremos clic sobre la carpeta a cifrar con el botón derecho del ratón y elegiremos la opción **Propiedades**. A continuación, en la pestaña **General**, pulsaremos en **Opciones avanzadas**. Para cifrar el contenido de la carpeta, haremos clic en **Cifrar contenido para proteger datos**. Luego, elegiremos si solo queremos cifrar esa carpeta o también las que contiene. A partir de ahora, otros usuarios del ordenador o de la red con los que compartamos la carpeta no podrán abrir los ficheros (aunque sí tendrán la opción cuáles son los que la integran).

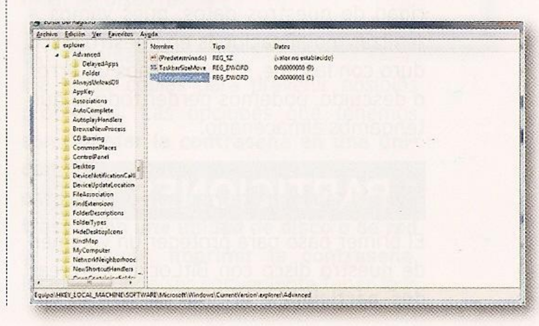


PASO 2
»TEN ACCESIBLES LAS CLAVES EFS

Para prevenir posibles problemas y que perdamos la posibilidad de abrir carpetas cifradas con EFS por, por ejemplo, errores en disco, tendremos la oportunidad de exportar las claves EFS. Al crear la carpeta con encriptación EFS, el sistema ofrecerá la alternativa de exportar el certificado. De este modo, aunque se deterioren los datos de usuario, podremos acceder a ellos importando el certificado original. Cuando aparezca el programa gestor de certificados, elegiremos la carpeta **Personal** y, a continuación, **Certificados**. Seleccionaremos nuestro nombre de usuario con el botón derecho y elegiremos la opción **Exportar**. Justo después, un asistente nos guiará en el proceso de la creación de la copia de los certificados de nuestro usuario. Al final del proceso, protegeremos la copia con una palabra clave y elegiremos un nombre para el fichero. Para importar un certificado almacenado, ejecutaremos el programa **certmgr.msc** en el **buscador del menú de Inicio**, haremos clic en la opción **Acción**, luego en **Todas las tareas** y, finalmente, en **Importar**. Comenzará el asistente de importación de claves al que le proporcionaremos el nombre del fichero que contiene clave y la contraseña.

PASO 3
»AGREGA LA OPCIÓN DE CIFRADO

Podremos agregar la opción de cifrado para que aparezca directamente en el menú de contexto cuando hagamos clic con el botón derecho sobre una carpeta. Para activar esta opción, ejecutaremos el Editor del archivo de Registro ejecutando **regedit** en la línea de comando dentro del **Menú inicio**. Luego, localizaremos la clave **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced** y crearemos una valor **DWORD** con el nombre **EncryptionContextMenu** y anotaremos **1**. A partir de ese instante, podremos cifrar la carpeta directamente desde el menú de contexto de las carpetas. ■



ENCRIPTA TU UNIDAD DE DISCO CON UNA MEMORIA FLASH USB

BITLOCKER PARA VISTA

Esta herramienta constituye una aplicación avanzada que permite encriptar unidades de disco utilizando una llave USB de forma que sean totalmente ilegibles .

BITLOCKER ES UNA POTENTE utilidad de encriptación disponible en **Windows Vista Ultimate**, **Windows Vista Enterprise** y **Windows Server 2008**. Permite la **protección de volúmenes de disco** a cuyos datos no podremos acceder a menos que seamos un usuario autorizado. Este sistema utiliza el algoritmo de encriptación AES en modo 128 bits. BitLocker puede funcionar en tres modos. El **transparente** no requiere ninguna acción por parte del usuario legítimo para acceder al disco, pero necesita que la placa base del ordenador disponga de un **chip TPM**. Este componente, identificado de forma única, actúa antes del arranque del sistema operativo para permitir el acceso al disco duro protegido. La segunda es la **autentificación por parte del usuario**, que también usa el chip TPM, pero, además, solicita que se introduzca una contraseña. Finalmente, está la opción que vamos a describir a continuación, la de la **llave USB**. En este caso, este dispositivo de memoria se transforma en una verdadera llave, ya que el sistema no arrancará a menos que esté insertada en una ranura USB antes del encendido.

Para que esta alternativa funcione, comprobaremos que la BIOS de nuestro ordenador permita el arranque desde un dispositivo USB. Antes de empezar, es conveniente realizar una copia de seguridad de nuestros datos, pues vamos a realizar modificaciones en nuestro disco duro con las que, si cometemos un error o descuido, podemos perder todo lo que tengamos almacenado.

»PARTICIONES

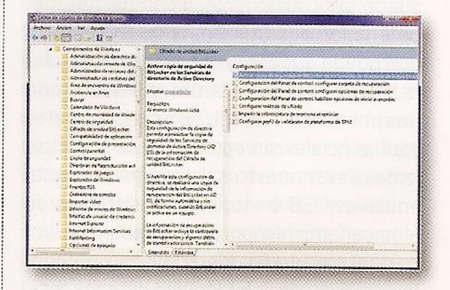
El primer paso para proteger un volumen de nuestro disco con BitLocker es crear **dos particiones**, la primera será el **volumen del sistema**. Éste contiene la información de arranque en un espacio no cifrado. La segunda será la que contenga el **sistema operativo y nuestros datos** protegidos por BitLocker.

PASO 1 »BITLOCKER DRIVE PREPARATION TOOL

Para configurar las particiones de forma que puedan funcionar con BitLocker, hemos de realizar la creación de las particiones a mano utilizando el disco de instalación de Windows Vista, pero es un proceso engorroso. Si queremos simplificar el proceso, podemos acudir a una utilidad específica diseñada por Microsoft. Para descargarla, acudiremos al símbolo de **Inicio** y escribiremos **Windows Update**. En la ventana que aparece, haremos clic en la parte izquierda, en **Busca actualizaciones**. Luego, al pinchar en **Ver actualizaciones disponibles**, descubriremos en la lista esta utilidad. También podemos descargarla directamente desde la página web **www.microsoft.com/downloads**, localizando el programa con la función de búsqueda. Enseguida, ejecutaremos la herramienta, que realizará los cambios en las particiones de manera automática.

PASO 2 »LOCALIZA LAS OPCIONES

Para configurar el comportamiento de BitLocker sin TPM, tendremos que abrir el Editor de directivas. Para ello, haremos clic en el icono de **Inicio** y escribiremos **gpedit.msc** en la casilla **Iniciar búsqueda**. Luego, pulsaremos la tecla **Enter** para ejecutar el **Editor de directivas de grupo local**. A continuación, pulsaremos dos veces con el ratón sobre **Configuración del equipo** para desplegar las opciones si no están ya visibles. Entonces, nos encaminaremos a **Plantillas administrativas** y buscaremos la opción **Componentes de Windows**. Accederemos a ella con un doble clic. Aquí, abriremos la opción **Cifrado de unidad BitLocker**.



PASO 3 »CONFIGURACIÓN DE BITLOCKER

Ahora, buscaremos la entrada **Configuración del Panel de control: habilitar opciones de inicio avanzadas** y la abriremos haciendo doble clic. En la ventana que se muestra, pulsaremos sobre la opción **Habilitada**. Si no disponemos de hardware compatible con TPM o queremos utilizar

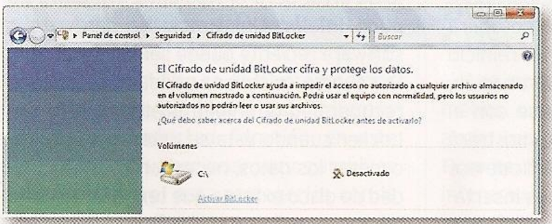
una unidad USB para el acceso, activaremos la casilla **Permitir BitLocker sin un TPM compatible** que se encuentra en la parte central del cuadro de diálogo. Algo más abajo, seleccionaremos las entradas **Permitir al usuario crear u omitir en las opciones Configurar opción de clave de inicio con TPM** y **Configurar opción de NIP de inicio con TPM**. De esta forma, será posible elegir en todo momento si queremos iniciar el equipo sin contraseña o con ella.

PASO 4 »ACTIVA LA CONFIGURACIÓN

Para que la configuración que hemos modificado se active inmediatamente, cerraremos el Editor de directivas de grupo local. A continuación, haremos clic en el icono de **Inicio**, escribiremos **gpupdate. exe /forceen** y, luego, pulsaremos **Enter**. De otro modo, las modificaciones realizadas no surtirán efecto hasta que se reinicie el sistema o apaguemos y encendamos el ordenador.

PASO 5 »ACTIVACIÓN DE BITLOCKER

Para activar la función de BitLocker, acudiremos a la configuración de seguridad del sistema operativo. Para ello, haremos clic en el icono de **Inicio** y, luego, sobre **Panel de control** y **Seguridad**. Si aparece el mensaje **Control de cuentas de usuario**, comprobaremos que la opción propuesta es la



que queremos. Rápidamente, abriremos la opción **Cifrado de unidad BitLocker**. En la ventana que se lanza, pulsaremos en **Activar BitLocker** en el volumen que corresponde al sistema operativo.

PASO 6 »INICIALIZA EL TPM

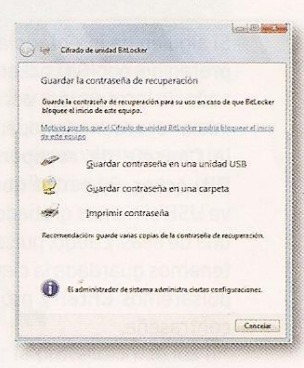
Si no hemos elegido la opción de utilizar una llave USB en el **Paso 3**, aparecerá el mensaje **Inicializar el hardware de seguridad de TPM**. Se trata del proceso de activación del chip TPM de la placa base del equipo para que pueda funcionar con BitLocker. Seguiremos las instrucciones del asistente y lo cerraremos con **Aceptar**. Reiniciaremos el equipo para que el sistema TPM de nuestro ordenador se ponga en marcha para seguir utilizando BitLocker.

PASO 7 »OPCIONES DE INICIO DE BITLOCKER

Si hemos tenido que reiniciar el sistema, volveremos al **Panel de control**, **Seguridad y Cifrado** de la unidad BitLocker para volver a activar la función. Si vamos a iniciar con una llave USB, insertaremos la llave en la ranura correspondiente (debe estar vacía). Luego, elegiremos **Requerir llave USB en cada inicio**, con lo que se mostrará en pantalla **Guardar clave de inicio.** Al pulsar sobre **Guardar**, el sistema almacenará las claves en la llave USB. A partir de ahora, es nuestra llave de acceso para el ordenador, por lo que tendremos mucho cuidado de no perderla.

PASO 8 »ALMACENA LA CONTRASEÑA

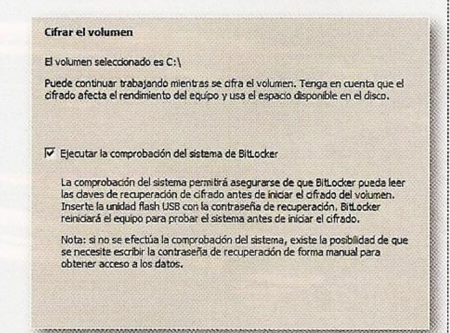
Después se nos presentará en pantalla el paso **Guardar contraseña de recuperación**. Ésta es muy importante porque es la que nos permite acceder al disco si está bloqueado por BitLocker ante un acceso no autorizado o cuando movemos el disco a otro sistema. Es recomendable hacer copias para prevenir posibles problemas. Las opciones que tenemos son **Guardar la contraseña en una unidad USB**, **Guardar la contraseña en una carpeta que nos permite guardar la contraseña en una unidad de disco o de red** y, finalmente, **Imprimir la contraseña**. Incluso, puede ser conveniente tener la ▶



password guardada de varias formas, aunque es importante conservar las copias a buen recaudo para que nadie tenga acceso a ellas sin autorización.

PASO 9
»INICIA EL CIFRADO

El siguiente paso es el del cifrado de la unidad de disco. Comprobaremos que está activada la opción **Ejecutar la comprobación del sistema de BitLocker** y pulsaremos en **Continuar**. Para que los cambios tengan algún efecto, pulsaremos sobre **Reiniciar ahora**. El equipo comprobará que BitLocker puede controlar el reinicio del sistema. Si se supera la comprobación, el disco comenzará a encriptarse con el mensaje **Cifrado en curso** y se mostrará el progreso de esta acción. A partir de ese momento, siempre que tengamos insertada la unidad USB con la clave de cifrado en el caso de que el equipo no sea compatible con TPM, el ordenador se iniciará en la forma habitual. Si se produce un intento de acceso no autorizado, tendremos que realizar el proceso de recuperación de datos protegidos.

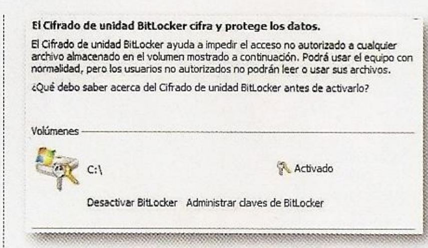


PASO 10
»RECUPERA DATOS DE BITLOCKER

Si alguien ha intentado acceder a un disco protegido por BitLocker o si hemos activado la protección por equivocación, al iniciar el ordenador aparecerá en pantalla la **Consola de recuperación de unidad BitLocker**. Se pedirá que se inserte la llave USB si hemos grabado la contraseña en una de ellas. Luego, pulsaremos **ESC**. Si no tenemos guardada la clave en la llave USB, pulsaremos **Enter** y proporcionaremos la contraseña.

PASO 11
»DESACTIVA BITLOCKER

Para desactivar la protección de BitLocker del volumen de la unidad que está protegida, seguiremos la ruta **Inicio/Panel de control y Seguridad** y volveremos a abrir la opción **Cifrado de unidad BitLocker**. Una vez en este punto, pincharemos en la opción correspondiente en el volumen protegido. Luego, podemos elegir entre descifrar el volumen o deshabilitar el cifrado, según lo que necesitemos.



»REPARACIÓN DE UNA UNIDAD BITLOCKER

En alguna ocasión, el disco duro puede fallar y afectar a la encriptación BitLocker del volumen, por lo que el equipo mostrará un mensaje de error y no podremos iniciar el sistema operativo ni siquiera conociendo la contraseña o insertando la llave USB correspondiente. Normalmente, el mensaje de error será el siguiente: **Windows no pudo iniciar**. Un cambio de hardware o software reciente puede ser la causa.

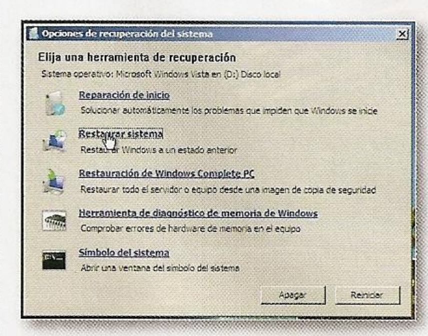
Por suerte, existe una utilidad que permite recuperar una unidad protegida con BitLocker cuando ésta se deteriora. Para recuperar los datos, necesitaremos una unidad de disco externa que tenga un tamaño igual o superior al disco duro que pretendemos recuperar. En ésta se almacenarán los datos recuperados.

PASO 1
»PREPARACIÓN DE LA UTILIDAD BITLOCKER REPAIR TOOL

Al igual que en el Paso 1 de la encriptación con BitLocker, buscaremos la utilidad correspondiente en la página de descargas de Microsoft **www.microsoft.com/downloads**. Si buscamos la clave **BitLocker** aparecerá la herramienta (**BitLocker Repair Tool**) que buscamos y la podremos descargar. Luego, copiaremos los siguientes ficheros en una unidad extraíble: **C:\Windows\system32\repair-BDE.exe, C:\Windows\system32\en-US\repair-BDE.exe.MUI**.

PASO 2
»INICIA EL SISTEMA

Como nuestro sistema no dispone de disco de arranque, utilizaremos el DVD de instalación de Windows. Para ello, activaremos la opción de arranque a partir del DVD de la BIOS e insertaremos el disco de instalación. Luego, en la página **Instalar Windows**, escogeremos **Reparar el equipo**.



Seguiremos las instrucciones del asistente y, cuando se nos presente la oportunidad, nos decantaremos por **Elegir una herramienta de recuperación** y haremos clic en **Símbolo de sistema**.

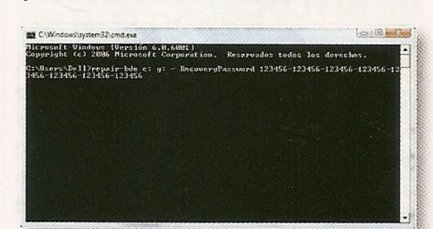
PASO 3
»LOCALIZA UNIDADES DAÑADAS

Para saber qué unidades son las dañadas, acudiremos al símbolo del sistema y escribiremos **Diskpart** y, cuando surja el símbolo del programa, escribiremos **List volume**. Aparecerá entonces una lista de particiones y volúmenes. Localizaremos el volumen con problemas, que será el que tenga como sistema de ficheros **RAW**, pues BitLocker no utiliza un sistema de ficheros habitual.



PASO 4
»REPARA EL VOLUMEN

Para iniciar la reparación, escribiremos el nombre de unidad donde estén almacenados los ejecutables que hemos copiado en la unidad Flash. Luego, escribiremos **repair-BDE unidad dañada unidad de recuperación – RecoveryPassword clave numérica**. Sustituiremos la **unidad dañada** por la letra de la unidad dañada. **Unidad de recuperación** es el disco duro externo en el que almacenaremos los datos recuperados. **Clave numérica** será la que hemos apuntado en el Paso 8. Luego, seguiremos las instrucciones para comprobar la integridad del volumen utilizando **chkdsk**.



MULTIMEDIA PRIVACY KEEPER NOS PERMITE SER SELECTIVOS

EL CIFRADO DE FOTOS Y VÍDEOS

A veces no interesa proteger unidades enteras, sino ciertos ficheros, como fotografías y vídeos personales. Lo conseguiremos con Multimedia Privacy Keeper.





MULTIMEDIA PRIVACY KEEPER
Contacto: Power Of Software
www.photopos.com/PPPKeeperLiteInfo.asp
UBICACIÓN EN EL DVD
Completos

SI LO QUE QUEREMOS proteger de ojos indiscretos no son los datos de nuestro ordenador de trabajo, sino cosas personales, tales como instantáneas o vídeos familiares, nuestra biblioteca de música..., podemos utilizar una herramienta específica para no tener que cifrar unidades enteras sino únicamente los ficheros que interesan. Para ello, acudiremos al programa Multimedia Privacy (**www.photopos.com/PPPKeeperLiteInfo.asp**).

PASO 1 »LOCALIZA LOS FICHEROS A CIFRAR

Una vez puesto en marcha el programa, seleccionaremos qué archivos multimedia queremos proteger con clave. Para ello, acudiremos al menú **File** y marcaremos **Browse Photos, Video and Audio Files** o haremos clic directamente en el icono que lleva el nombre **Browse**. Aparecerá un mensaje solicitando una contraseña. Simplemente, pulsaremos sobre **Cancel** para acceder a la lista de ficheros del sistema. Localizaremos la carpeta que contiene los archivos que queremos proteger en la parte inferior. En la zona derecha, veremos una previsualización del contenido. Podemos escoger un fichero o varios manteniendo pulsada la tecla **Control**.

PASO 2 »ASIGNA UNA PALABRA CLAVE

Una vez elegido el fichero/s a encriptar, pulsaremos el **icono del candado** en la parte superior del menú. Entonces se lanzará una ventana en la que agregaremos más a través de **Add files** o los quitaremos con **Remove selected**. También, en este caso, podemos seleccionar varios archivos pulsando **Control** para protegerlos con la misma contraseña. Una vez tengamos la lista de ficheros definida, pulsaremos en el campo **Password** para asignar una palabra clave. A continuación, tendremos que repetir la contraseña en **Confirm password**. Finalmente, haremos clic en **Next**.

PASO 3 »ASOCIA INFORMACIÓN FALSA

Este programa permite asociar información falsa al fichero que protegemos. En caso de que así sea, accedermos a una ventana que nos permitirá buscar otro fichero multimedia que se mostrará en lugar del original. En la parte inferior, podremos elegir entre dos opciones: que se muestre directamente un **fichero falso** cuando se abra el archivo desde Windows o con el programa, pero dando una clave errónea (para no hacer ver que el fichero está protegido); o despistar, aún más, **protegiendo la visualización del fichero falso con una clave adicional**. Para elegir el archivo falso, haremos clic en **Add files** y, luego, en **Next**. Tendremos que confirmar la protección de los ficheros seleccionados desde **Protect**. En la lista de archivos de la parte inferior izquierda de la ventana, veremos el nuevo aspecto de la previsualización de los mismos. Como precaución adicional, es conveniente cambiar el nombre de los ficheros.

PASO 4 »VISUALIZA EL CONTENIDO PROTEGIDO

No se podrá acceder a esos ficheros a menos que abramos el programa. Para abrir el contenido original, haremos clic en **Browse**, localizaremos el fichero que nos interesa y pincharemos sobre él. Veremos en el área de previsualización el **icono de un candado** sobre la imagen. Para visualizar el contenido protegido, cerraremos el



programa. Al volver a abrirlo y pulsar en **Browse**, nos solicitará una contraseña. Podremos previsualizar los ficheros protegidos con ella, que se mostrarán con un **icono rodeado del color verde**.

PASO 5 »QUITA LA PROTECCIÓN

Si queremos quitar la protección de los ficheros, los seleccionaremos y haremos clic en el **icono del candado con un aspa roja**. El programa nos solicitará la palabra clave y su confirmación. Para terminar, pulsaremos **Next** y, finalmente, **Remove protection**. Luego, borraremos los *dummies* que se han creado en el directorio donde hemos desprotegido las imágenes. ■

UNA ALTERNATIVA A LOS SISTEMAS DE CODIFICACIÓN DE WINDOWS

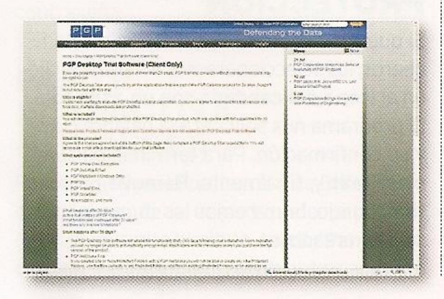
CAMUFLA TU INFORMACIÓN

Si no disponemos de una versión de Windows con BitLocker o queremos utilizar un sistema alternativo, Pretty Good Privacy Desktop puede ser la solución más adecuada y potente.

LA ENCRIPTACIÓN PGP (*Pretty Good Privacy*) es uno de los sistemas más populares en la Red para proteger los datos. Permite distintas funciones, pero veremos solo las de cifrado. En este sentido, puede ser una buena alternativa, incluso más potente, a las soluciones de encriptación que ofrece Windows y que hemos visto anteriormente. Con PGP es viable **configurar una unidad virtual cifrada y encriptar una partición completa con claves de 256 bits**. El programa se distribuye desde la página web de PGP en versión de prueba. Al cumplir 30 días algunas funciones dejan de funcionar, aunque puede seguir utilizándose el sistema de cifrado/descifrado de ficheros.

PASO 1 »DESCARGA E INSTALACIÓN

Para descargar el software, acudiremos a la web **www.pgp.com/downloads/desktoptrial/desktoptrial2.html**, donde aceptaremos el contrato de licencia y rellenaremos un formulario. Así, nos enviarán al correo electrónico un enlace para iniciar la descarga. La instalación se efectúa con un asistente que nos pedirá el número de licencia (anotado en un documento PDF adjunto al correo electrónico con el enlace de descarga). El asistente de instalación se pondrá en marcha cuando reiniciemos el sistema.



PASO 2 »CONFIGURACIÓN DE LA CLAVE

Tras la instalación del programa, aparecerá un **icono** en la parte derecha de la barra de tareas **en forma de candado**. Para acceder a la interfaz principal, tendremos que hacer doble clic sobre ese icono. Una vez abierto, procederemos a crear una clave de cifrado. Éstas son las que luego permitirán encriptar y desencriptar los datos y unidades. Para generar una nueva clave, encaminaremos nuestros pasos a **File/**



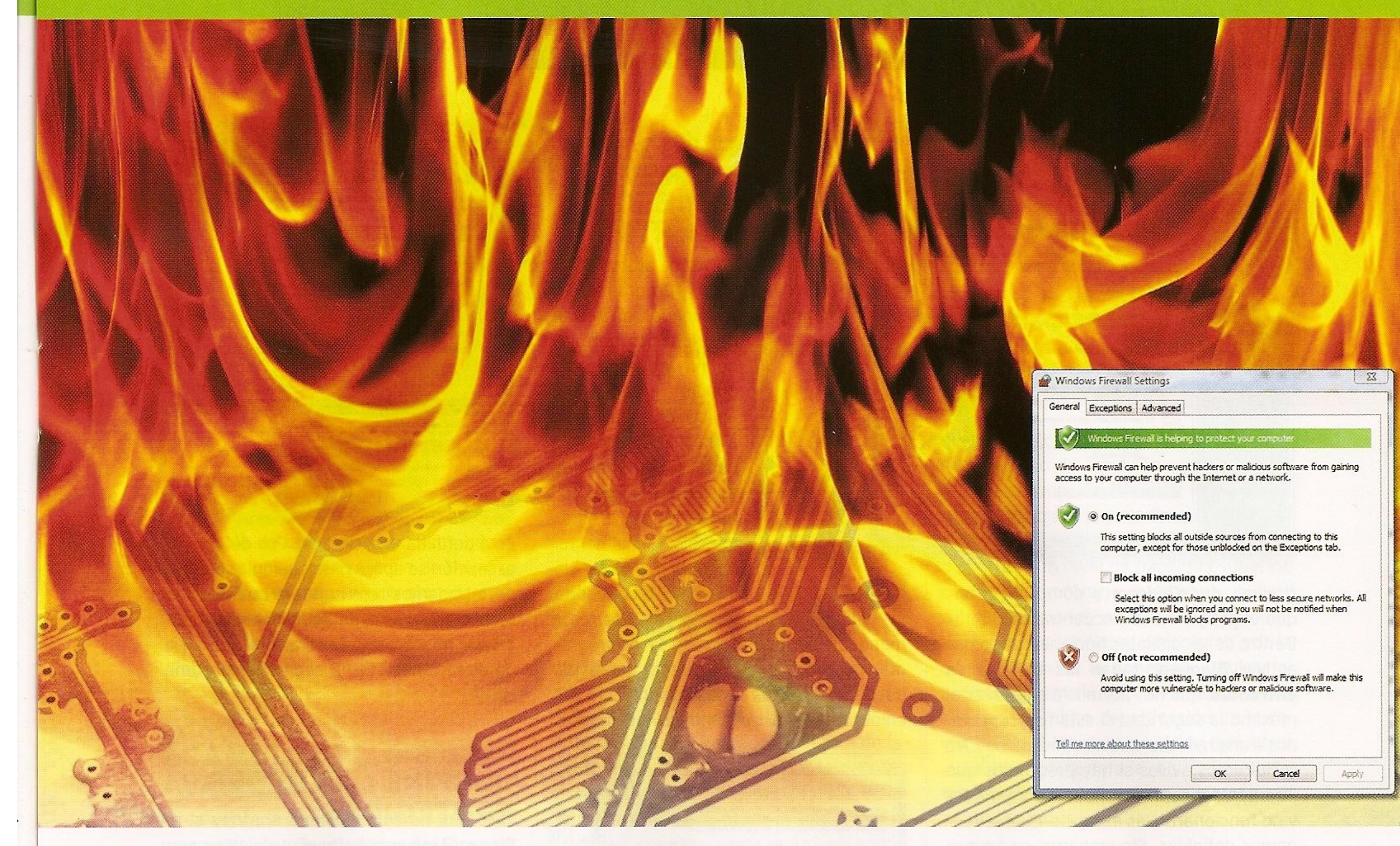
New PGP Key. Se abrirá el asistente de generación de claves PGP, que nos solicitará el nombre y el correo electrónico. Es necesario que cada clave está asignada a un usuario de forma única. Para la generación de la clave, en **Enter passphrase**, introduciremos una frase clave que repetiremos para confirmar. Al pulsar en **Siguiente**, se generará la *password* que nos corresponde. Como no vamos a utilizar por ahora la clave para el correo electrónico, en el último paso, **PGP global directory assist**, pulsaremos **Skip**. En la ventana principal, en nuestro **Keyring** (llavero), aparecerá la contraseña generada. Con ella ya podemos comenzar a encriptar.

PASO 3 »ENCRIPTA FICHEROS COMPRIMIDOS

Con PGP es posible crear un fichero comprimido en el que incluir distintos archivos que quedarán protegidos por una clave PGP. Haremos clic en **PGP Zip** y se desplegarán más opciones. Pulsando en **New PGP Zip**, aparecerá una ventana en la que podremos arrastrar y soltar los archivos que vamos a comprimir y proteger. Si marcamos la opción **Send original files to PGP Shredder when finished**, los ficheros originales se someterán a un proceso de borrado seguro.

Si pulsamos en **Siguiente**, nos presentarán cuatro alternativas. La primera sirve solamente si se tiene un par de claves, la del creador del fichero y la del destinatario. Si el uso del fichero es para nosotros, tendremos que crear una clave nueva. Es la opción más segura. La segunda supone que los receptores del fichero no tiene clave pero sí PGP Desktop y la palabra clave. La tercera solicita una clave, pero no precisa que los usuarios del fichero usen PGP Desktop para la descompresión. La última, simplemente, firma el archivo ZIP con nuestra clave PGP sin encriptarlo. Si elegimos la segunda o la tercera opción, nos pedirá una palabra clave, que será la que utilizaremos para desencriptar el fichero. Luego, escogeremos nuestra clave para codificar el archivo y se completará el proceso.

Como hemos apuntado, cabe la posibilidad de utilizar el programa PGP para encriptar un disco entero. Este proceso es bastante parecido al apuntado en el Paso 3, pero hay que tener en cuenta que, pasados los 30 días de prueba, el disco se desencriptará automáticamente. ■



DESCUBRE LAS BARRERAS DE WINDOWS VISTA PARA INTERNET

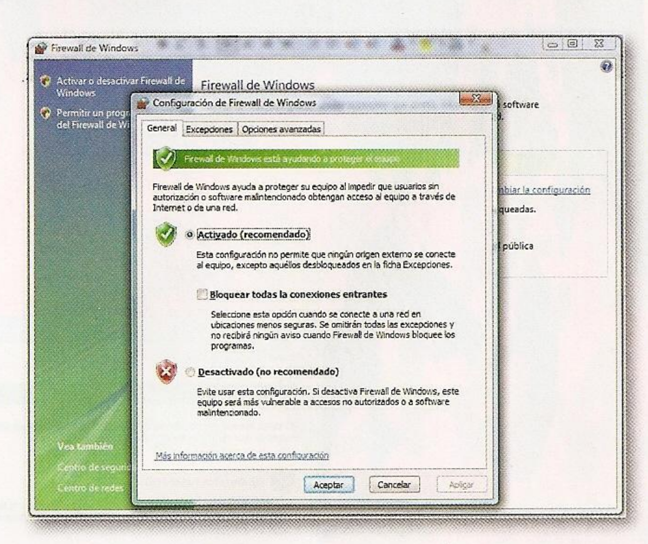
EL FIREWALL DE MICROSOFT

Otra de las herramientas de seguridad que proporciona de serie la última edición de Windows es el cortafuegos capaz de interceptar conexiones entrantes y salientes.

UN CORTAFUEGOS ES una herramienta que permite controlar la conexión a Internet e **interceptar conexiones tanto salientes como entrantes que accedan a puertos y recursos no autorizados**. De esta forma, se bloquean de raíz cualquier ataque externo y cualquier conexión desde dentro que pueda suponer un envío de información no autorizado. Hay que tener en cuenta que, además de protegernos, estos programas, si no son configurados correctamente, pueden hacer que dejen de funcionar ciertas aplicaciones que se conectan a Internet. Los *firewalls* pueden estar alojados en distintos sitios, desde el sistema operativo hasta el *router* o incluso un dispositivo que funcione como *firewall* directamente conectado a Internet. En ocasiones, incluso se utiliza una combinación de estos. En algunas empresas se emplean no solo para atajar problemas de seguridad, sino para limitar servicios que no se desea que utilicen los trabajadores. En Windows Vista, se incorpora un programa de cortafuegos básico que podemos configurar para que nuestras aplicaciones trabajen correctamente. Hay que tener en cuenta que es posible que tengamos que modificar la configuración del programa según vayamos instalándolas.

PASO 1 »ACTIVA EL CORTAFUEGOS

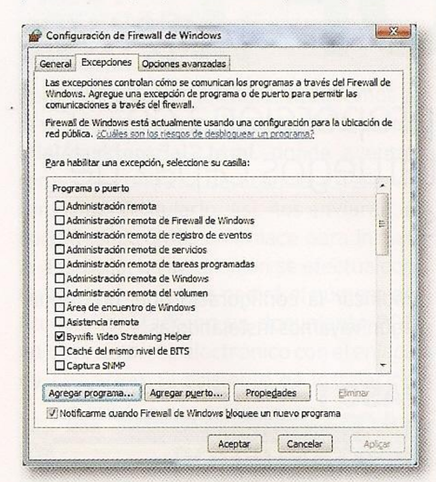
Como decíamos, dentro de las herramientas de seguridad de Vista, se incluye un programa que hace las funciones de cortafuegos. Para acceder a éste, iremos a **Inicio/Panel de control/Seguridad/Firewall de Windows**. Una vez abierta la ventana, haremos clic en **Activar o desactivar** ▶



firewall de Windows y comprobaremos que el programa se encuentra habilitado. Dentro de las distintas opciones, podemos activar **Bloquear todas las conexiones entrantes**, que nos permitirá aumentar al máximo la seguridad si estamos conectados a una red local que no conozcamos. No recibiremos avisos si hay programas que intentan conectar con nuestro ordenador y no funcionarán las excepciones que tengamos definidas. Sin embargo, podremos navegar y utilizar los programas de correo electrónico.

PASO 2
»PERMITE EL ACCESO DE PROGRAMAS

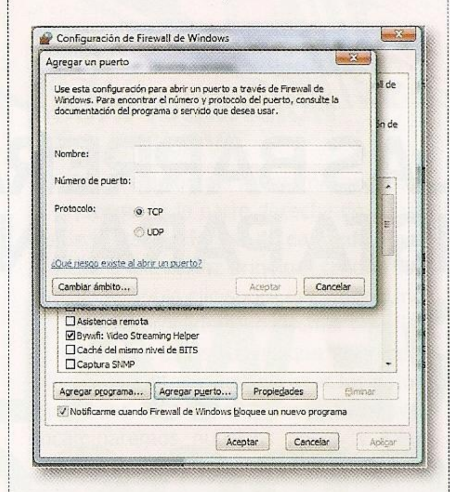
Podemos permitir que ciertos programas puedan acceder a la red o bloquearlos activando la opción **Permitir un programa a través del Firewall de Windows**. Se mostrará una lista de aplicaciones de las que podemos agregar una excepción para un



programa o desactivarlo. Si queremos añadir una nueva aplicación a la lista, haremos clic sobre **Agregar programa**. También tenemos la oportunidad de definir si queremos o no que Windows nos advierta cada vez que el *firewall* localiza un software con acceso a Internet y lo bloquea.

PASO 3
»ADMITE EL ACCESO A PUERTOS

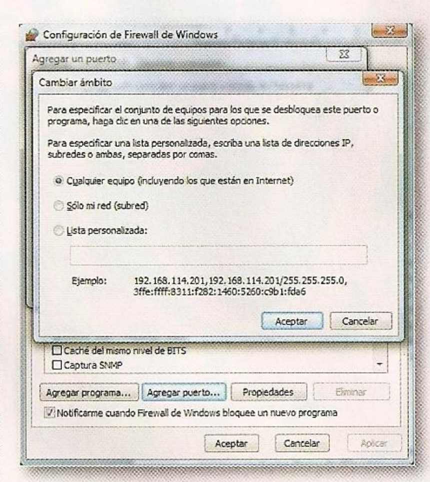
En vez de otorgar permisos a programas determinados, el *firewall* de Vista nos permite definir a qué puertos pueden acceder las aplicaciones para salir a Internet. De esta manera, limitaremos las posibilidades de conexión de un programa sólo parcialmente, habilitando parte de los puertos que utiliza pero bloqueando los peligrosos. Sin embargo, es más recomendable permitir el acceso de los programas que abrir puertos, puesto que estos quedan expuestos desde que los abrimos en el *firewall* hasta que lo deshabilitamos.



Sin embargo, al posibilitar el acceso a un programa, este sólo permanecerá abierto durante el tiempo en el que el esté activo y utilice la conexión. Para permitir el acceso a un puerto siempre, dentro de la ventana que hemos abierto en el Paso 2, haremos clic en **Agregar Puerto**. Es importante que demos un nombre a la excepción para poder identificarla con el software que la utiliza. Tenemos la opción de abrir dos tipos de puertos: **TCP** o **UDP**. Es conveniente comprobar qué tipo y número de puerto precisa exactamente nuestro programa. Para cada uno de ellos es posible que nos pida abrir más de un puerto.

PASO 4
»DEFINE EL ÁMBITO

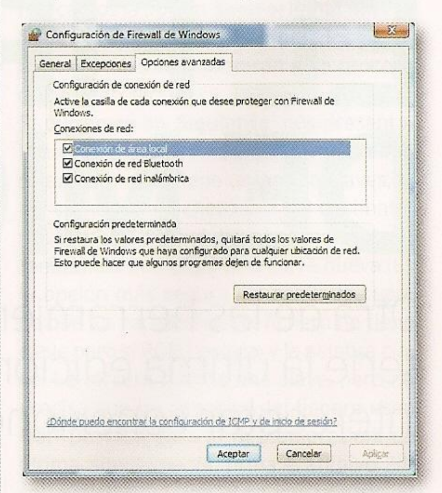
Tanto en el Paso 2 como en el Paso 3, en la ventana para permitir el acceso a un programa o puerto, aparece un botón llamado **Cambiar ámbito**. Esta opción sirve para restringir los equipos para los que



está definida la excepción. Por defecto, la excepción se aplica para cualquier equipo, pero podemos restringirlo a **nuestra red local** o a una **lista de equipos especificada por nosotros**. Esta lista será una serie de direcciones TCP/IP separadas por una coma.

PASO 5
»DEFINE LAS REDES PROTEGIDAS

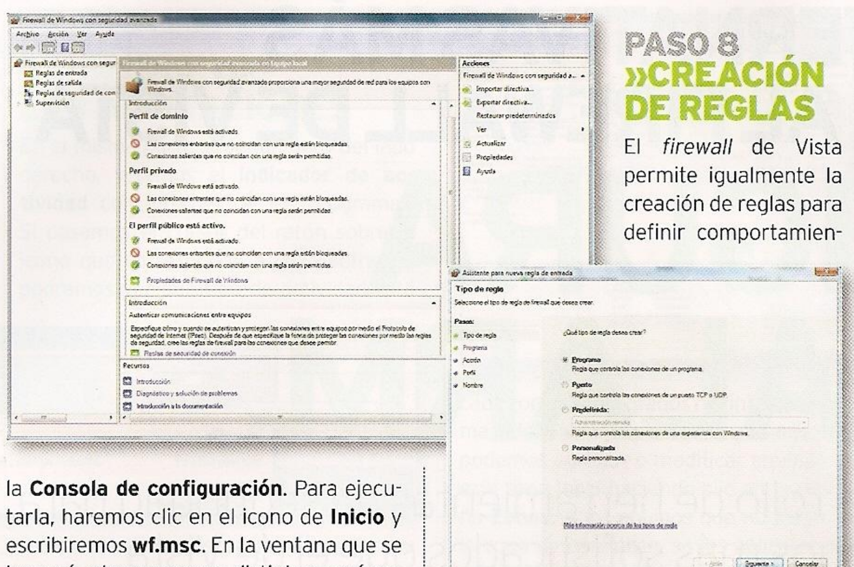
En la ventana del *firewall* de Windows, podremos definir opciones más avanzadas haciendo clic en **Cambiar la configuración**. Accederemos nuevamente a las opciones del *firewall* y pincharemos en la pestaña **Opciones avanzadas**. Dentro de ella, encontraremos la posibilidad de de-



terminar para qué tipo de redes a las que accede el ordenador queremos que actúe el cortafuegos. Por último, es factible restaurar los valores por defecto del *firewall* haciendo clic en el botón correspondiente.

PASO 6
»CONFIGURACIÓN AVANZADA DESDE LA CONSOLA

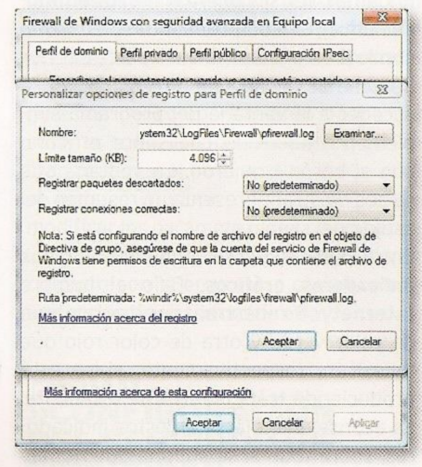
Para configurar opciones avanzadas del *firewall* de Vista, tendremos que activar



la **Consola de configuración**. Para ejecutarla, haremos clic en el icono de **Inicio** y escribiremos **wf.msc**. En la ventana que se lanzará, observaremos distintos parámetros y configuraciones del cortafuegos de Windows Vista.

PASO 7 »CAMBIA OPCIONES AVANZADAS

En la ventana que tenemos en pantalla, haremos clic en **Propiedades del Firewall de Windows**, de modo que se nos presente una nueva ventana donde modificar la configuración. Podemos **bloquear o permitir las conexiones entrantes y salientes**. Si queremos limitar a través del mismo las conexiones de otros usuarios



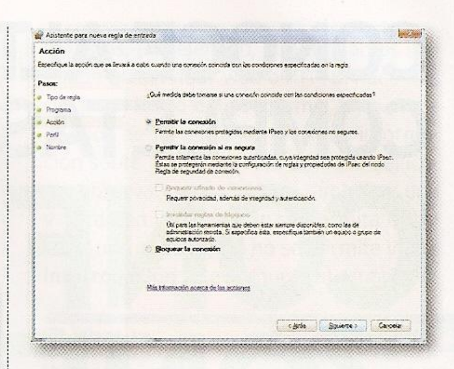
del ordenador, es posible bloquear las salientes. En la configuración del **perfil de dominio**, tenemos la opción de activar o desactivar el que se muestren mensajes a los usuarios cuando intenten acceder con un programa o a un puerto no autorizados. En las opciones de registro del perfil de dominio, definiremos un sistema para que se grabe un **archivo** en el que se quedarán **almacenadas las conexiones fallidas o exitosas**. Puede ser útil para detectar comportamientos extraños que pueden delatar la presencia de *malware* en el sistema.

PASO 8 »CREACIÓN DE REGLAS

El *firewall* de Vista permite igualmente la creación de reglas para definir comportamientos fijos para la protección de las conexiones. Para conseguirlo, desde la ventana de **Firewall de Windows**, basta con seleccionar **Reglas de entrada** en la lista de la parte izquierda y, posteriormente, el enlace **Nueva regla** en la lista de tareas de la parte derecha para iniciar el asistente. En este caso, crearemos una regla para admitir las comunicaciones al navegador. Así, marcaremos la opción **Programa** de la lista de opciones y pulsaremos en **Siguiente**. Seleccionaremos la opción **Esta ruta de acceso del programa**, pincharemos en **Examinar** y buscaremos en el Explorador el ejecutable del programa. Por último, hay que pulsar el botón **Siguiente** de nuevo.

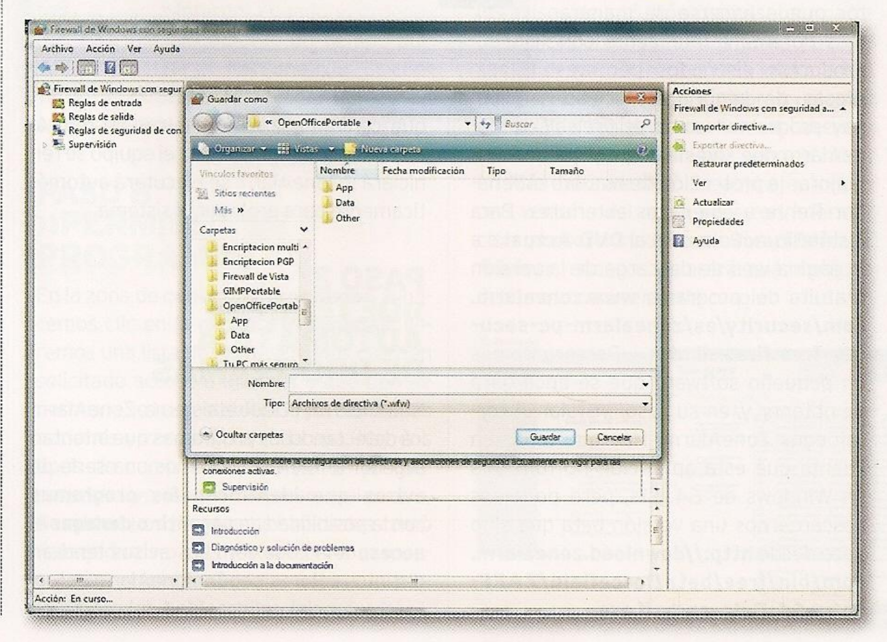
PASO 9 »PERMISOS DE CONEXIÓN

En la siguiente pantalla del asistente de configuración, hay que concretar la medida que debe tomar el *firewall* en función del tipo de conexión que se vaya a producir. La opción **Permitir la conexión si es segura** asegura la identidad del emisor mediante el sistema **Ipsec**, por lo que ofrece un nivel de fiabilidad superior, pero, por el contrario, puede que muchas de las conexiones no se puedan completar. Lo más sencillo es decantarse por la opción **Permitir la conexión** y pulsar el botón **Siguiente**. La próxima ventana nos plantea el ámbito de aplicación de la regla. En el último paso, solo hay que introducir un **nombre** para la regla y una corta **descripción**. Para terminar, pulsaremos el botón **Finalizar**.



PASO 10 »EXPORTA DIRECTIVAS

Una vez hayamos establecido la configuración del *firewall*, podremos grabar un archivo para exportar la configuración. Con ello, tendremos una copia de seguridad o podremos configurar otros equipos de la red de idéntica manera. Para hacerlo, sencillamente haremos clic en la parte derecha de la ventana y en **Exportar directiva**. Justo después, elegiremos un **nombre de fichero** y lo guardaremos. Luego, podremos recuperar la directiva con la opción **Importar directiva**.



CONOCE ALTERNATIVAS MÁS COMPLETAS AL FIREWALL DE VISTA

CONFIGURA ZONEALARM

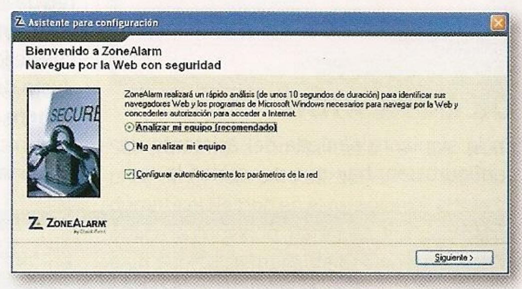
Las empresas de desarrollo de herramientas de seguridad para PC producen cortafuegos más sofisticados que el de Vista. ZoneAlarm es un buen ejemplo.



LA HERRAMIENTA DE FIREWALL incorporada a Windows Vista es suficiente para un usuario básico y con pocas necesidades. Sin embargo, el proceso de controlar las conexiones entrantes y salientes, establecer reglas, comportamientos, bloquear de forma condicional programas y puertos puede hacerse de manera más potente e inteligente con productos diseñados por empresas de seguridad. Incluso, hay programas como el *firewall* de ZoneAlarm que son sin coste y que pueden mejorar la protección de nuestro ordenador frente a amenazas exteriores. Para instalarlo, acudiremos al **DVD Actual** o a la página web de descarga de la versión gratuita del programa **www.zonealarm.com/security/es/zonealarm-pc-security-free-firewall.htm.** Descargaremos un pequeño software que se encargará de obtener y, en su caso, instalar el cortafuegos ZoneAlarm. Hay que tener en cuenta que esta aplicación no funciona en Windows de 64 bits, pero podemos descargarnos una versión beta que sí lo hace desde **http://download.zonealarm.com/bin/free/beta/forcefield/ZAFF-Setup64-Beta-en-bzff.exe.**

PASO 1 »COMPROBACIONES INICIALES

Durante la instalación, ZoneAlarm efectuará una serie de comprobaciones y ajustes de seguridad que serán importantes para la configuración del *firewall* más adelante. Al principio del proceso de instalación, el asistente nos ofrece la posibilidad de que **el programa identifique los navegadores y otras aplicaciones de Windows para permitirles automáticamente el acceso a la red.** Igualmente, indica si queremos



que configure los parámetros de red. Al terminar la comprobación, el equipo se reiniciará y ZoneAlarm se ejecutará automáticamente para proteger el sistema.

PASO 2 »DETECCIÓN AUTOMÁTICA DE PROGRAMAS

Nada más reiniciado el sistema, ZoneAlarm irá detectando los programas que intentan acceder a Internet. Veremos una serie de **avisos que identifican los programas** con la posibilidad de **permitir o denegar el acceso** a la conexión. Los avisos tendrán distintos **colores según** ZoneAlarm detecte la potencial **peligrosidad** del programa que intenta acceder. Una vez terminado el arranque, comprobaremos que las herramientas que utilizamos normalmente y que acceden a Internet funcionan de forma correcta ejecutándolas. Si no es así, tendremos que definir permisos manualmente, como veremos más adelante.

PASO 3 »CONTROL DEL TRÁFICO

Podemos ver si ZoneAlarm está en funcionamiento comprobando si el **icono con la Z** se encuentra en la parte inferior derecha de la barra de tareas. Es posible acceder a la ventana del programa simplemente haciendo clic sobre el icono con el botón izquierdo. La ventana que se nos mostrará presenta un resumen del estado del sistema.

En la parte superior, podemos ver **dos indicadores gráficos.** Bajo el nombre **Internet** se muestran dos barras, una de color verde y otra de color rojo que muestran, respectivamente, si se está produciendo **tráfico entrante o saliente.** Es aconsejable fijarse en estos indicadores, sobre todo si se supone que no hay ningún programa en funcionamiento que debería acceder a Internet. Junto a los indicadores se muestra un **botón rojo** que brinda la posibilidad de bloquear de forma instantánea el acceso a la Red. Una función útil si sospechamos que se están produciendo accesos no autorizados.



PASO 4
»CONTROL DE LAS APLICACIONES

En la misma parte superior, pero del lado derecho, veremos el **indicador de actividad** con Internet de los programas. Si pasamos el cursor del ratón sobre el icono que corresponde a cada software, podremos ver qué tipo de actividad está



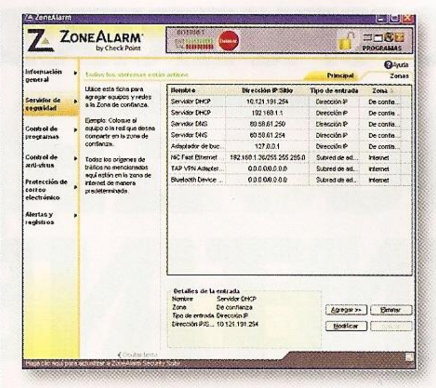
realizando. Eso nos permitirá vigilar su comportamiento por si no fuera el que se espera. El **icono de candado** colocado a la izquierda de los de los programas, posibilita bloquear todo acceso a Internet. Podremos definir más detalles sobre los programas que acceden a Internet en la sección de ZoneAlarm correspondiente.

PASO 5
»ESTADO DEL SISTEMA

En la parte central de la ventana principal, se muestra el estado del sistema de protección. Aparecen todos los intentos de **intrusiones bloqueadas**, **cuántos programas están accediendo al exterior con autorización** y el estado de la **protección del correo electrónico**. En la pestaña **Preferencias**, podemos cambiar la configuración del comportamiento básico del sistema, como la comprobación de actualizaciones o si el programa se carga o no al iniciarse Windows. También es posible modificar los parámetros de protección de identidad cuando el software se ponga en contacto con la empresa o el sistema de protección de *password* de **eBay**.

PASO 6
»CONFIGURACIÓN DEL SERVIDOR DE SEGURIDAD

Si hacemos clic en la parte izquierda de la ventana, sobre **Servidor de seguridad**, podremos modificar el comportamiento del sistema de protección del tráfico. Éste tiene configuradas dos zonas de seguridad: la local o **zona de confianza** y la de **Internet**. Se aplican reglas distintas para las conexiones dependiendo de la zona en la que se encuentre el ordenador definido por su dirección IP. La **zona de confianza**, normalmente, la forman los equipos y dispositivos de nuestra red local. El programa permite ajustar el nivel de protección de



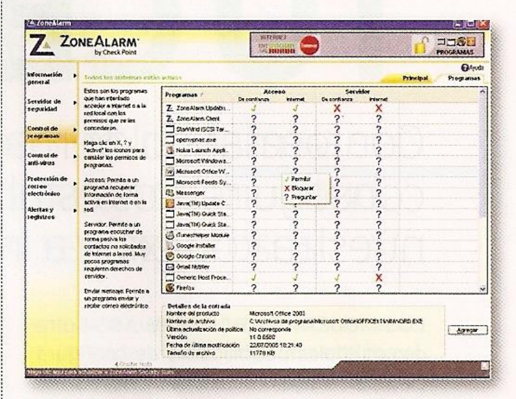
cada zona en tres grados distintos y de forma independiente para cada una. Además, podemos agregar o modificar equipos de este área local haciendo clic en la pestaña **Zonas**. A los equipos que no estén en la zona de confianza, se les aplicarán las reglas de la **zona Internet**.

PASO 7
»NIVELES DE CONTROL

Si hemos observado que un programa que utilizamos no dispone de acceso a Internet desde que instalamos ZoneAlarm o por el contrario hemos visto que un programa que dispone de acceso se comporta de forma extraña al monitorizarlo en la pantalla principal, podemos cambiar la configuración de cómo se controla a los programas haciendo clic en la sección **Control de programas**. Como puede leerse en la pantalla de información, ZoneAlarm recomienda dejar el control de programas en nivel **Medio** los primeros días de funcionamiento. Una vez que hayamos utilizado todas nuestras aplicaciones habituales, lo recomendable es definir el nivel **Alto** de protección. El **bloqueo automático** lo activaremos cuando vayamos a dejar el ordenador desatendido. Esta función bloquea todo acceso a Internet cuando el ordenador está inactivo durante un tiempo que podemos definir en **Personalizar**. Es conveniente establecer al mismo tiempo un salvapantallas protegido con *password*.

PASO 8
»PERMISOS DE PROGRAMAS

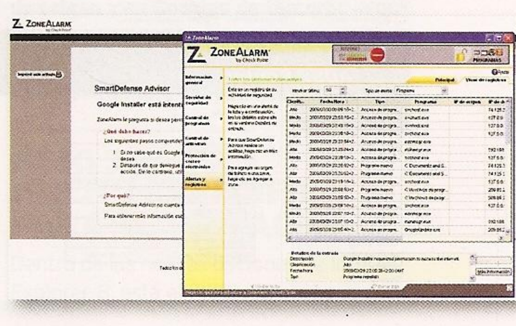
En la zona de **control de programas**, si hacemos clic en la pestaña **Programas**, veremos una lista de los desarrollos que han solicitado acceso a Internet y qué tipo de permisos se han establecido para distintas acciones y zonas. Para cada una, hay dos tipos de comportamiento de un programa, el activo, llamado **Acceso**, y el pasivo, **Servidor**. Los programas habituales como navegadores o clientes de correo o mensajería instantánea son normalmente activos, pocos se comportan como servidores, a menos, por ejemplo, que tengamos instalado un servidor web o FTP. Si hacemos clic en el **icono del programa**, en la parte inferior de la ventana, veremos información sobre el mismo. A la derecha del icono, observaremos distintos símbolos: una **v** verde en caso de que se permita el acceso, una **aspa roja** si no se permite y **una interrogación** si se pregunta al usuario so-



bre si permite el acceso. Podemos eliminar software haciendo clic con el botón derecho y eligiendo la opción correspondiente o agregarlo si aún no está en la lista.

PASO 9
»REGISTRO DE ACTIVIDAD

Es factible controlar cómo ha funcionado ZoneAlarm y qué actividad se ha producido en la red accediendo a la zona de **Alertas y registros**. En la ventana principal, podemos definir cómo y con qué frecuencia se recogen los datos. Si hacemos clic en la pestaña **Visor de registros**, visualizaremos los registros de actividad. En el menú desplegable **Tipo de alerta**, podremos seleccionar si queremos ver el registro de la actividad del programa o del servidor de seguridad, donde encontraremos los avisos de intrusión o acceso por parte de aplicaciones potencialmente peligrosas. Si deseamos recibir más información por parte de ZoneAlarm sobre cualquier entrada del registro de actividad, haremos clic sobre ella y pulsaremos sobre el ratón en **Más información.** Se abrirá entonces una ventana del navegador con información proporcionada por **SmartDefense Advisor**, que nos aclarará qué medidas debemos tomar en cada caso. ■



CONTROLA LA PUERTA DE ENTRADA

EL ROUTER, TU CENTINELA

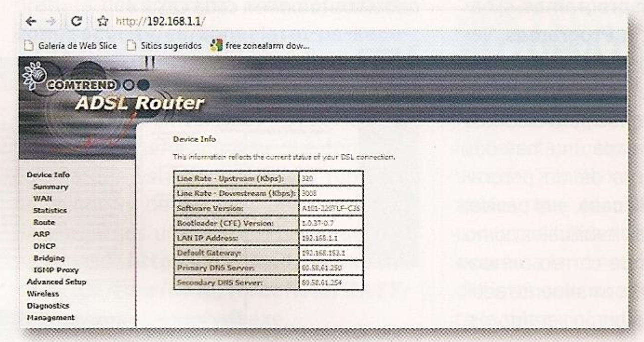
Conformando de manera adecuada nuestro router ADSL, conseguiremos establecer la primera barrera de seguridad en nuestra conexión a Internet.

LOS MODERNOS ROUTERS ADSL ofrecen múltiples posibilidades de configuración para atajar conexiones indebidas de raíz, antes incluso que lleguen a nuestro ordenador. Prácticamente, todos estos dispositivos modernos permiten el filtrado de los accesos a Internet, ya sea a través de la **función NAT** como mediante un sistema de *firewall* completo. En ocasiones, es posible que, al intentar utilizar aplicaciones como **eMule**, programas de juego *on-line* o telefonía IP y, a pesar de tener configurado el cortafuegos del sistema operativo para que permita su funcionamiento, el software no logre acceder a los puertos correspondientes de forma correcta. El principal sospechoso, en este caso, será precisamente el *router*, y tendremos que acceder a su configuración para abrir dichos puertos y permitir el funcionamiento de los programas.

PASO 1 »ACCESO A LA CONFIGURACIÓN

En ocasiones, los proveedores de acceso a Internet proporcionan un programa con el que podemos abrir los puertos del *router* que están cerrados por defecto y realizar modificaciones en los parámetros de seguridad. Sin embargo, en muchos casos, tendremos que acceder a su configuración directamente a través del navegador web.

En efecto, estos dispositivos disponen normalmente de un pequeño servidor al que podemos acceder con un navegador de Internet y así cambiar las variables oportunas. En primer lugar, tendremos que saber qué **dirección IP** se asigna el *router* dentro de la red local y a continuación conocer qué **usuario** y **contraseña** tiene configurados para conformar los parámetros correspondientes. Esa información la suele tener el proveedor de acceso, aunque podemos acudir a páginas como **www.adslayuda.com** y buscar la marca y modelo de nuestro dispositivo para obtener dichos datos. Una vez estemos en posesión de la dirección IP, la introduciremos en el navegador. Luego, visitaremos la página de acceso a la configuración con el usuario y contraseña asignados. Los *routers*, salvo excepciones, como los últimos modelos de **Cisco Linksys**, no suelen tener funciones avanzadas de *firewall*, sino que simplemente se limitan a bloquear el acceso a las peticiones de los puertos desde el exterior. Normalmente, la seguridad está activada al máximo en el *router*. Lo comprobaremos en cualquier caso accediendo a la configuración y comprobando si el **firewall** y el **bloqueo de puertos** están activados.

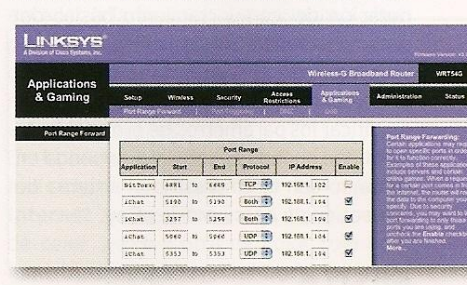


PASO 2 »PUERTOS POR NAT

Para abrir los puertos por defecto bloqueados en un *router*, accederemos a la configuración avanzada y, luego, al apartado **NAT**. El nombre del apartado que nos permitirá abrir los puertos correspondientes bloqueados por el *firewall* por defecto suele ser **Port triggering** o similar. Una vez accedamos a éste, podremos agregar nuevos perfiles asociados a las aplicaciones que precisan puertos abiertos. En el caso del *router* del ejemplo, estamos limitados a **32 excepciones**. Agregaremos una excepción pulsando en **Add**. En este caso, el *router* tiene algunas aplicaciones predefinidas que podremos elegir con un menú desplegable. Si la aplicación no se encuentra entre las listadas, habrá que agregar a mano el rango de puertos a abrir y el tipo de los mismos.

PASO 3 »TRADUCCIÓN DE PUERTOS

Para que otras utilidades como **eMule** funcionen de forma óptima, tendremos que



acceder también a la configuración de conversión de direcciones que puede llamarse **Virtual Servers**, **Address mapping**, **Port fordwaring...** Esta función permite que el tráfico que llega de determinados puertos desde Internet sea entregado a la IP interna de la red local.

Lo configuraremos de forma similar a lo que hemos hecho en el apartado anterior. Para evitar que otras aplicaciones utilicen esta puerta de entrada a través de los puertos, se recomienda deshabilitar el acceso una vez hayamos terminado con la aplicación que los utiliza. Para conocer detalles de la configuración, acudiremos al manual del programa que precisa la apertura de los puertos. ■

AJUSTA BIEN SUS OPCIONES
EL NAVEGADOR MÁS FIABLE

Hace tiempo que los navegadores han dejado de limitarse a ser meros escaparates para las páginas web, ejecutando multitud de programas y complementos que podrían ser peligrosos.



LOS NAVEGADORES SON la puerta de entrada de Internet, la herramienta más utilizada para acceder a la Red. Nos permiten no solamente acceder a las páginas web, sino también ejecutar aplicaciones, *scripts* y complementos. Además, intercambian información con las páginas almacenando datos de navegación y sirven de vehículo para transmitir información confidencial, como datos bancarios
Todas estas aplicaciones hacen que un navegador sea un objetivo preferente para los desarrolladores de *malware* o *hackers* que quieran obtener nuestros datos. Por eso, poco a poco, estas aplicaciones han ido incorporando complementos de seguridad para ir enfrentándose a los retos que se han ido presentando en Internet.

Un navegador más seguro

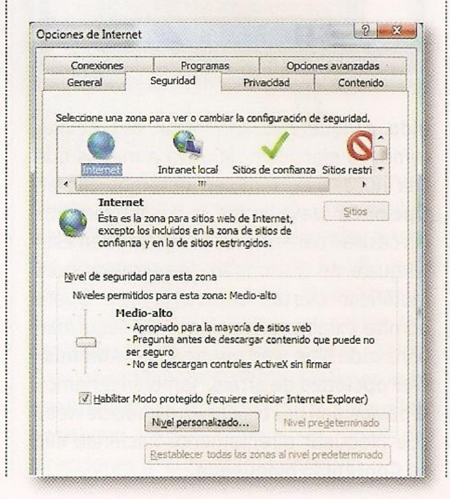
La primera medida para disponer de un navegador seguro es que esté actualizado. Hoy en día, los productos de Windows suelen comprobar por su cuenta el estado de actualizaciones y avisan al usuario o las descargan automáticamente para que las vulnerabilidades que hayan podido aparecer queden resueltas. Los tipos de ataque a los que están expuestos se relacionan con las extensiones y las posibilidades que ofrecen y que multiplican sus vulnerabilidades. Hablamos de los controles ActiveX, programas en Java, *plug-ins*, *cookies*... Quizás los más vulnerables son los lenguajes de *script*, como Javascript o VBScript. Vamos a ver, navegador por navegador, qué opciones podemos activar para aumentar la seguridad y la privacidad.

»SEGURIDAD CON IEXPLORER 8

La última entrega del navegador de Microsoft dispone de una completa serie de medidas de seguridad que se han incorporado para adaptarse a las nuevas amenazas procedentes de Internet.

PASO 1 »OPCIONES DE SEGURIDAD

Al igual que en la versión anterior, IE 8 permite modificar el nivel de seguridad de navegación según las cuatro zonas de navegación predefinidas. Para acceder a esta configuración, haremos clic en **Herramientas/Opciones/Seguridad**. En la ventana que aparece, seleccionaremos la zona de la que nos interese cambiar el nivel de protección y, luego, moveremos el indicador hasta obtener la protección deseada. En el nivel de seguridad más alto, desactivaremos controles ActiveX, Active Scripting y Java. Si pulsamos en **Nivel personalizado**, podremos determinar qué componentes se controlan o se impide su funcionamiento. Algunas páginas web, sobre todo aplicaciones *on-line*, podrían no funcionar con el nivel de protección más alto, pero es el más seguro para la navegación. Para aquellas páginas web en las que confiemos y para las que necesitemos tener activados los controles, añadiremos su dirección web a la zona de **sitios de confianza** haciendo clic sobre el icono correspondiente y luego en **Sitios**.



PASO 2 »CONFIGURA LAS COOKIES

Las *cookies* entregan información sobre nuestra navegación y otros datos a los sitios que las utilizan. Podemos configurar un control más estricto de ellas acudiendo a **Herramientas/Opciones/Privacidad**, donde veremos un indicador de nivel de privacidad parecido al del punto anterior. Para hacer que el navegador pregunte siempre que se graba una *cookie* y pida confirmación, haremos clic en **Avanzada**, luego, en **Invalidar la administración automática** y, finalmente, estableceremos en **Cookies de origen** y en **Cookies de terceros** la opción **Preguntar**. Para que no recibamos un exceso de notificaciones, activaremos **Aceptar siempre las cookies de sesión**.

PASO 3 »MENÚ ESPECÍFICO PARA TU PRIVACIDAD

Dentro de las nuevas opciones de Internet Explorer 8, está el modo de navegación ▸



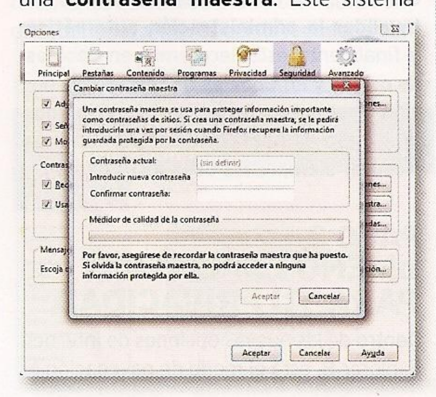
Inprivate, que impide que se almacenen datos sobre la navegación. También permite deshabilitar extensiones y barras de herramientas. Podemos acceder a este tipo de navegación privada haciendo clic en **Seguridad/Exploración de Inprivate**. Otras funciones interesantes son el borrado selectivo del historial de navegación, el **filtro Inprivate** o el **filtro Smartscreen**, que utiliza una amplia base de datos de páginas web peligrosas para prevenirnos de posibles problemas.

»SEGURIDAD EN FIREFOX

Es el segundo navegador más popular que crece por momentos en número de usuarios. Una de sus principales vulnerabilidades es también una de sus principales bazas: la abundancia y calidad de complementos disponibles. Hay que ser muy cuidadosos a la hora de instalar estos *plug-ins*. También dispone de un navegador en modo privado que se instala por separado llamado **Mozilla Firefox (modo seguro)**.

PASO 1 »OPCIONES DE SEGURIDAD

Todose controla desde el menú **Herramientas/Opciones/Seguridad**. Para evitar que los sitios web instalen complementos sin nuestro consentimiento, comprobaremos que está activada la opción **Advertir cuando un sitio intente instalar componentes**. Podremos añadir sitios de confianza pulsando el botón **Excepciones**. Otra opción conveniente es la de utilizar una **contraseña maestra**. Este sistema hace que Firefox encripte toda la información confidencial, como contraseñas y nombres de usuario, y la proteja con una palabra clave.



PASO 2 »COMPLEMENTOS Y ACTUALIZACIÓN

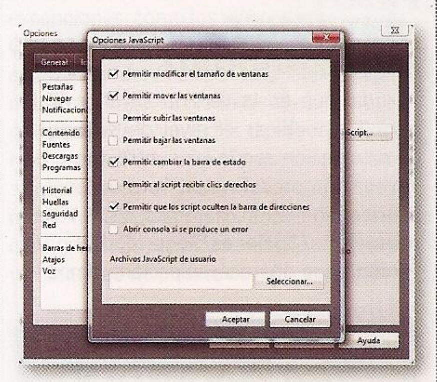
Si pulsamos en el icono **Contenido**, podremos desactivar o configurar en qué condiciones se van a ejecutar los distintos complementos. Se recomienda visitar el apartado **Avanzado**, junto a **Activar Javascript**, y desactivar todas las casillas que veamos en la ventana. Otra precaución que aconsejamos es desactivar la ejecución de programas Java, a menos que sean indispensables. Y si es necesario activar esta función, anular la activación una vez se ha ejecutado el programa que precisemos.

»SEGURIDAD EN OPERA

Otro de los navegadores más populares que contempla opciones para el control de complementos y también de las *cookies*, en este caso llamadas **huellas**.

PASO 1 »OPCIONES DE SEGURIDAD

Podemos controlar la descarga y ejecución de los complementos y programas de Opera abriendo **Herramientas/Opciones/ Avanzado** y buscando la sección **Contenido**. Al igual que en Firefox, deshabilitaremos la ejecución de Java a menos que sea necesario. También haremos clic en **Opciones Javascript** y desactivaremos las casillas para que los programas en este lenguaje no dispongan de permisos para modificar ciertas características. Opera admite establecer opciones de seguridad para cada sitio web pulsando en **Administrar opciones de sitios**. También tenemos la posibilidad de realizar un listado de webs que bloquear directamente haciendo clic en **Contenido bloqueado**.



»SEGURIDAD EN GOOGLE CHROME

El nuevo navegador presentado por Google ha demostrado ser uno de los más seguros, quizás también porque lleva menos tiempo en activo y, por lo tanto, los desarrolladores de *malware* no han tenido tiempo para aprovechar brechas de seguridad. Por defecto, el navegador dispone de un sistema de detección de páginas web peligrosas que nos avisará si visitamos una dirección no recomendable.

PASO 1 »NAVEGACIÓN DE INCÓGNITO

Al igual que Internet Explorer 8 y Firefox, Chrome también permite un modo de navegación, llamado **Incógnito**, que no deja rastros de información en las páginas web que visita. Para abrir una página del navegador en esta modalidad, podemos acudir al menú de herramientas (el **icono de la herramienta**) y elegir la opción correspondiente o pulsar **Control + Mayúsculas + N**.

PASO 2 »DESACTIVA JAVA Y JAVASCRIPT

Google Chrome no dispone por defecto de la posibilidad de desactivar aplicaciones Java o JavaScript. Para conseguirlo, tendremos que lanzar el programa con parámetros. Localizaremos el **icono de Chrome** y haremos clic sobre el mismo con el botón derecho para pulsar sobre **Propiedades**, y copiaremos el contenido del campo **Destino** con **Control + C**. Luego, acudiremos al icono de **Inicio** y pulsaremos **Control + V** para copiar la ruta del programa. Entonces, añadiremos tras la ruta completa **-disable-javascript** o **-disable-java**, según la característica que queramos deshabilitar. También podemos crear un acceso directo para ejecutar el programa con estas características. Para volver a habilitar las funciones, repetiremos la operación, pero con la palabra **enable**. ■



SALVAGUARDA TU RED WIRELESS

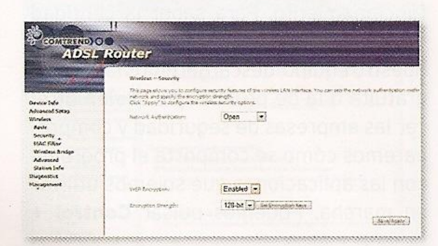
PRECAUCIONES PARA TU WIFI

Uno de los puntos más sensibles de las redes locales es la conexión inalámbrica WiFi, ya que cualquiera dentro de su alcance puede interceptarla e introducirse en tu entorno.

LAS REDES INALÁMBRICAS han sido siempre objeto de ataques para acceder a la red local u obtener sin permiso acceso a Internet. Al tratarse de una red a la que no es necesario conectarse físicamente, el peligro de un acceso no autorizado es grande, por lo que es obligado tomar medidas preventivas. Para ello, hay que recurrir a la configuración del *router*.

CONSEJO 1
»SISTEMA DE CLAVES

El primer error que se suele cometer al configurar una red inalámbrica es la de no establecer un sistema de encriptación y contraseña. De este modo, cualquiera podrá conectarse y utilizar sus recursos. Para activar la **encriptación**, que puede ser **WEP o WPA**, accederemos a la configuración del *router*, tal y como hemos visto en el práctico correspondiente, y activaremos esta función. En la configuración del dispositivo, estableceremos también la calidad de la encriptación y la contraseña para acceder a la red.



CONSEJO 2
»LA CONTRASEÑA DEL ROUTER

En muchas páginas web, circulan tanto el nombre de usuario como la contraseña que los distintos proveedores de acceso a Internet establecen para sus *routers*. Lo primero que tenemos que hacer cuando nos lo entreguen es cambiarla para que, si alguien accede a nuestra red, no modifique los parámetros de configuración.

CONSEJO 3
»EL NOMBRE DE LA ESTACIÓN BASE

Al igual que con el nombre de usuario y contraseña, para la configuración del *router* los proveedores de acceso proporcionan un nombre único para los que instalan. Es conveniente **cambiar ese nombre SSID** del *router* tanto para evitar confusiones como para no dar información del tipo de conexión que tenemos instalada.

CONSEJO 4
»EL FILTRADO MAC

La dirección MAC identifica de forma única todos los dispositivos de red. En los **routers inalámbricos**, podemos **establecer un filtrado** de modo que los dispositivos que no pertenezcan a la lista **de direcciones MAC** autorizadas no puedan acceder a la red. Así, será imposible que otros dispositivos externos entren sin nuestra supervisión y permiso. Sin embargo, no se trata de un sistema infalible, ya que algunos programas enmascaran la dirección MAC.

CONSEJO 5
»DESHABILITA EL SERVIDOR DHCP

Normalmente, los *routers* entregan direcciones IP automáticamente a cualquier dispositivo de la red que lo solicite a través del protocolo DHCP. Esto facilita que podamos conectar nuevos dispositivos a la red sin volver a configurar el *router*. No obstante, podemos desactivar esta opción como medida de seguridad y **asignar manualmente las direcciones IP a los dispositivos**. Estableceremos un rango de direcciones IP autorizadas para ello.

CONSEJO 6
»CONTRO DE ACCESOS

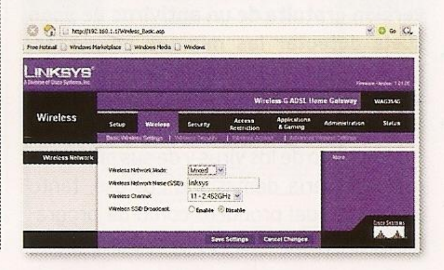
Algunos *routers* permiten el **control de los accesos a la red local a través de conexiones WiFi**. También podemos controlar los accesos en los archivos de entrega de direcciones IP por parte del servidor DHCP del *router*.

CONSEJO 7
»APAGA EL ROUTER

Cuando no lo utilicemos durante largos períodos de tiempo, hemos de **apagar el enrutador**. De esta forma, impediremos que nadie se conecte a nuestro dispositivo cuando no estemos presentes y podamos tomar medidas. Por otro lado, ahorraremos algo de energía eléctrica. El *router* no debería resentirse y, normalmente, no perderá la configuración.

CONSEJO 8
»NO A LA EMISIÓN DE LA DIRECCIÓN SSID

Nuestro *router* emite una señal para **identificarse como punto de acceso WiFi publicando su dirección SSID**. Esta función no es necesaria en una red local doméstica, por lo que la **deshabilitaremos** para que ni siquiera se conozca la presencia de nuestro dispositivo. Con todo, hay que tener en cuenta que existen programas especiales capaces de detectar los puntos de acceso, aunque no emitan su dirección SSID.



CÓMO ELEGIR Y CONFIGURAR EL ANTIVIRUS ADECUADO

UNA PIEZA FUNDAMENTAL

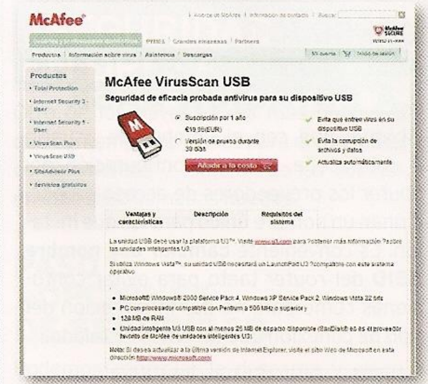
El antivirus es imprescindible cuando hablamos de la seguridad de nuestro ordenador. Es importante elegir el más adecuado y utilizarlo y configurarlo según nuestras necesidades.

LOS PROGRAMAS ANTIVIRUS se han hecho muy populares entre los usuarios de ordenador, ya que llevan muchos años entre nosotros protegiendo la integridad de nuestro PC. Si, al principio, el peligro eran los virus o troyanos, que inicialmente solo podían propagarse a través de disquetes que circulaban de un ordenador a otro, Internet ha multiplicado exponencialmente sus posibilidades de difusión pero también el tipo de *malware* o código malicioso que podemos encontrar en la Red.

Actualmente, los antivirus se han convertido en completas *suites* de seguridad, que no solo **protegen de amenazas de forma estática**, sino que **controlan los adjuntos** que llegan a nuestro **correo electrónico**, **comprueban las páginas web** que visitamos, **protegen del spyware** e incluso, en algunos casos, comprueban los enlaces de una página antes de que hagamos clic sobre ellos. El primer paso para disponer de una protección correcta es elegir un buen antivirus. Veamos cómo.

Gratuitos o de pago

A la hora de instalar un antivirus nos encontramos con una sorpresa: muchas empresas ofrecen, además de su software de seguridad de pago, versiones gratuitas. Incluso existen antivirus totalmente gratuitos. El eterno debate es si estas versiones protegen con la misma eficacia el ordenador que las de pago. En realidad, **una versión gratuita de un antivirus de pago suele detectar las mismas amenazas**. Una de las principales razones de que esto sea así es que a las empresas de seguridad les interesa recoger datos sobre el comportamiento de los virus y de sus antivirus. Además, sería demasiado costoso, tanto en imagen del producto como de programación, realizar una versión del programa que detectara solo parte de las amenazas. ¿Qué diferencia estas versiones gratuitas de las de pago? Por un lado, en algunos casos, la detección es igualmente potente, pero no lo es así el mecanismo de reparación de los archivos dañados. En otros, el programa gratuito detectará el archivo infectado y lo pondrá en cuarentena, pero solo podremos borrarlo o utilizar la versión de pago para limpiarlo. Cuidado que esto ocurre solamente en casos puntuales, ya que en muchas ocasiones el antivirus gratuito limpiará nuestro ordenador sin problemas. Por supuesto que, al adquirir la versión de pago, nos libraremos de avisos publicitarios y dispondremos de herramientas más cómodas y potentes, pero, en general, se puede decir que las versiones gratuitas protegen igual que las de pago.



• Existen antivirus específicos para situaciones concretas, como los nuevos para llaves USB, que protegen estas unidades de posibles problemas de forma automática sin necesidad de instalar programas en el PC.

¿Cuál es el mejor antivirus?

Es una pregunta muy peliaguda. En realidad, el mundo del *malware* es tan cambiante y con una velocidad tal que es imposible juzgar con precisión qué programa de antivirus es el más eficaz en todo momento. Instituciones como **AV Comparatives** ofrecen estudios periódicos con colecciones de *malware* en continua renovación basados en estadísticas de porcentajes de detección y de falsos positivos. Puede consultarse el resultado de estas comprobaciones en su web **www.av-comparatives.org**. Otra guía fiable son las comparativas de antivirus de PC Actual.

A la hora de escoger una *suite* de seguridad, nos fijaremos, por un lado, en la **eficacia del motor de antivirus y malware**, pero, por el otro, en factores como el **tipo de herramientas disponibles** y **cuántos recursos consume** cuando está en funcionamiento. Para saber la cantidad de recursos que consume el antivirus en nuestro equipo, descargaremos la versión gratuita o la de prueba que suelen ofrecer las empresas de seguridad y comprobaremos cómo se comporta el programa con las aplicaciones que solemos utilizar en marcha. Podemos pulsar **Control +**



• Los informes que miden la calidad del motor de detección de amenazas de los programas antivirus solo son una parte de las prestaciones en las que debemos fijarnos a la hora de elegir el software de seguridad adecuado.

Alt + Supr para iniciar el **Administrador de tareas** y tomar nota del uso de la CPU y de memoria del antivirus.

»CONFIGURACIÓN DEL ANTIVIRUS

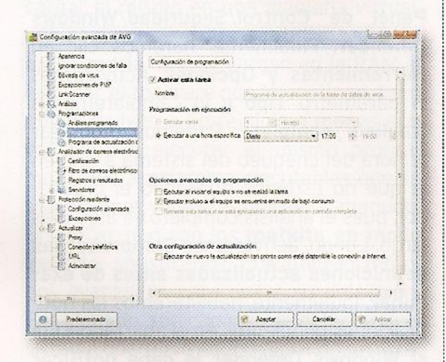
Para sacar el máximo partido de nuestra *suite* de seguridad, como en cualquier otro tipo de aplicaciones, es preciso ajustar la configuración a nuestras necesidades. A continuación, veremos cómo configurar las opciones más importantes en dos programas de antivirus: **AVG** en su versión gratuita y **Panda Antivirus 2009**, de pago. Los ajustes son similares en aplicaciones de otras marcas.

AVG antivirus gratuito

Podemos descargarlo desde la página web **http://free.avg.com**. El programa incluye antivirus, *anispyware*, analizador de correo electrónico, comprobador de seguridad de enlaces (**Link Scanner**) y protección residente.

PASO 1 »ACTUALIZACIONES AUTOMÁTICAS

Todos los programas antivirus suelen activar por defecto la actualización automática, que descarga tanto cambios en la aplicación como las nuevas listas de amenazas, que son las que permiten al antivirus ser eficaz. Para comprobar la frecuencia de las actualizaciones de AVG, haremos clic en **Herramientas** y en **Configuración avanzada**. Enseguida, Abriremos la sección **Programaciones** y,



dentro de ellas, encontraremos dos apartados: **Programa de actualización de la base de datos de virus** y **Programa de actualización del programa**. En esta versión, únicamente podremos activar las actualizaciones automáticas diarias y elegir la hora. Por precaución, en ambos apartados, es muy interesante activar la opción **Ejecutar al iniciar el equipo si no se realizó la tarea**. Si no estamos permanentemente conectados a Internet, también activaremos la opción de **Actualizar en cuanto se conecte**.

PASO 2 »ANÁLISIS AUTOMÁTICOS

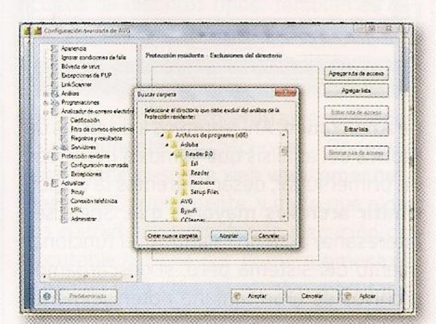
Aunque tengamos activado el sistema residente que bloquea ataques, es importante programar análisis periódicos para detectar posibles infecciones. Activaremos los análisis periódicos en la misma ventana que en el paso anterior, pero abriendo la opción **Análisis programado**. En primer lugar, activaremos el **Análisis automático**. Luego, programaremos la ejecución del análisis, según el uso que de-



mos al ordenador. Es útil activar también aquí la opción de **Ejecutar el análisis si no se realiza la tarea**. Por su lado, activar **Retrasar esta tarea si se está ejecutando una aplicación a pantalla completa** es conveniente para no perjudicar la ejecución de programas. En la pestaña, **¿Cómo analizar?**, elegiremos los procesos a realizar y la prioridad de los procesos. También es aconsejable activar los **Informes**.

PASO 3 »EXCEPCIONES

El sistema de detección de *malware* residente puede bloquear determinados programas, aunque no contengan amenazas.



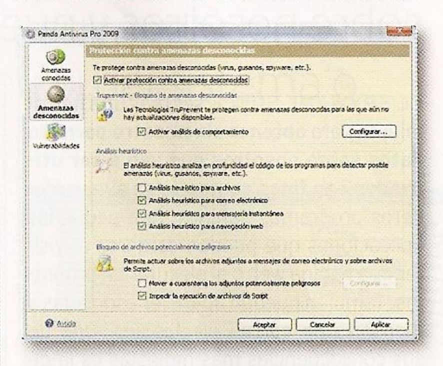
Si ocurre, podemos agregar excepciones al programa. En la ventana de **Configuración avanzada**, seguiremos la ruta **Protección residente/Excepciones**. Podemos agregar programas a las excepciones haciendo clic en **Agregar ruta de acceso**.

Panda Antivirus Pro 2009

Se trata de la última versión de la popular herramienta de seguridad de Panda, que dispone del nuevo sistema de detección llamado **Inteligencia Colectiva**, una tecnología que mejora la detección de *malware*, incluso en el caso de que sea desconocido, reduciendo la necesidad de ancho de banda y de recursos del sistema. Podemos descargar una versión de prueba en **www.pandasecurity.com**.

PASO 1 »CONFIGURACIÓN DEL COMPORTAMIENTO

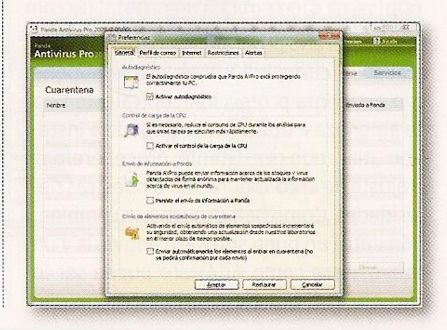
Es posible acceder a la configuración del antivirus desde **Antivirus**, en el apartado **Protecciones**. Aquí, tenemos la oportunidad de configurar el comportamiento del antivirus contra las amenazas conocidas



y definir el comportamiento de los análisis de cada herramienta del programa. También podremos concretar el *modus operandi* del antivirus ante amenazas desconocidas. Para aumentar la seguridad, activaremos el **análisis heurístico**.

PASO 2 »PREFERENCIAS DE SEGURIDAD

Habilitaremos otros parámetros de seguridad del programa haciendo clic en **Preferencias**, en la ventana principal. En la pestaña **General**, activaremos el **autodiagnóstico**, para que el propio programa detecte si está protegiendo correctamente al sistema. El **Control de carga de la CPU** ralentiza la ejecución del antivirus para otorgar más recursos al sistema. También es conveniente habilitar la opción de **enviar los archivos que ponga el programa en cuarentena** (es decir, supuestamente infectados) **para que sean analizados en los laboratorios de Panda.**



LAS UTILIDADES ANTISPYWARE
NO PERMITAS QUE TE ESPÍEN

Además de las amenazas clásicas, las páginas de Internet se han llenado de spyware, programas que recaban información sobre nosotros y nuestra navegación.

EL SPYWARE SUELE ser más una herramienta para **obtener sin nuestro permiso datos sobre nosotros que van a ser utilizados con fines comerciales** que verdaderos programas dañinos. Son pequeñas aplicaciones que pueden cargarse al visitar una página web o al ejecutar un programa. También pueden aparecer asociadas a mensajes de correo electrónico. Una de sus consecuencias más molestas es la de modificar el comportamiento de nuestro navegador. Algunos de estos programas provocan la **aparición de ventanas emergentes** o *pop-ups*, otros instalan barras de herramientas no autorizadas...

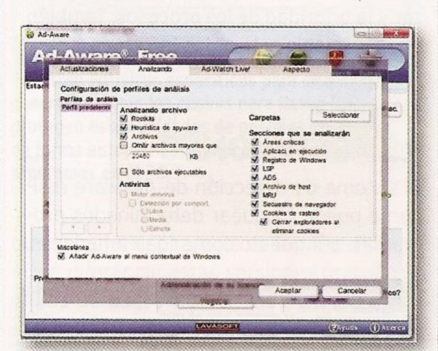
Uno de los síntomas más claros, además de la aparición de los apuntados, es que **la navegación se vuelve más lenta**. Las *suites* de seguridad y antivirus actualmente suelen incorporar una herramienta *antispyware*. Sin embargo, puede ser conveniente instalar una aplicación específica, que disponga de datos más actualizados. Además de programas gratuitos, como **AdAware**, que podemos descargar de la página **www.lavasoft.com**, Microsoft proporciona para los usuarios de Windows Vista y XP su propia herramienta. Se trata del programa **Windows Defender** y, si no lo tenemos instalado, lo podemos descargar de forma gratuita desde **www.microsoft.com/windows/products/winfamily/defender**. Vamos a ver cómo configurar una herramienta *antispyware*.

Trabaja con AdAware

Es un veterano programa *antispyware* que acaba de cumplir 10 años y que supone una excelente protección contra este tipo de amenazas. Una vez descargado e instalado utilizando el asistente, procederemos al ajuste de la configuración a nuestras necesidades. Como hemos dicho, la combinación entre un buen software antivirus y un *antispyware* como AdAware puede ser lo más eficaz. Para ejecutarlo, haremos doble clic en el **escudo rojo con fondo verde** que aparecerá en la barra de tareas.

PASO 1 »PERSONALIZA EL ANÁLISIS

Por defecto, AdAware establece unos ajustes de análisis que son adecuados para la mayoría de las situaciones. Sin embargo, recomendamos hacer algunos más para estar mejor protegidos. Obviamente, para variar los parámetros acudiremos al icono **Configuración** y pincharemos en la pestaña **Analizando**. Ahí, veremos los ajustes de fábrica del análisis que vamos a modificar. En primer lugar, desactivaremos la opción **Omitir archivos mayores que**. Suele ser interesante para no ralentizar el funcionamiento del sistema pero, si descargamos archivos de gran tamaño potencialmente peligrosos, es mejor desactivarla. En el apartado **Secciones que se analizarán**, escogeremos **Cerrar exploradores al eliminar cookies**.



PASO 2 »BORRA LOS RASTROS

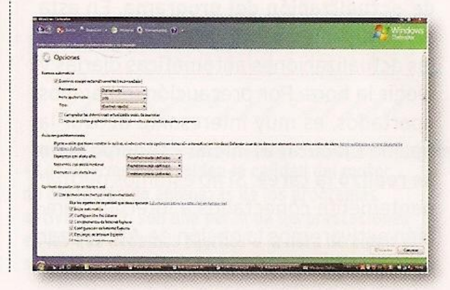
Una utilidad interesante incorporada en AdAware es **TrackSweep**, que permite eliminar todo rastro de navegación. Para acceder a ella, usaremos el icono de **Extras** de la parte superior derecha de la ventana (en forma de cruz) y elegiremos la pestaña **TrackSweep**. Observaremos toda la información que nos permite eliminar el programa y podremos desactivar ciertos procesos de borrado, por ejemplo, las *cookies* si utilizamos un servicio que precisa de esta funcionalidad. Luego haremos clic en **Limpiar ahora**.

Windows Defender

Este programa básico de Microsoft para la prevención ante *spyware* también permite la configuración de ciertos parámetros para mejorar su funcionamiento.

PASO 1 »CONFIGURACIÓN

Para manipular los ajustes, abriremos **Panel de Control/Seguridad/Windows Defender**. Finalmente, haremos clic en **Herramientas y Opciones**. Activaremos el parámetro **Tipo** y lo cambiaremos a **Análisis completo**. Podemos modificar la hora del chequeo del sistema a una en la que no estemos utilizando el ordenador, pues el análisis completo es algo más largo. Luego, activaremos **Comprobar las definiciones actualizadas antes de examinar**. Igualmente, habilitaremos las notificaciones pendientes en el apartado **Elija si Windows Defender le debe notificar sobre:**. En **Opciones avanzadas**, tenemos la posibilidad de agregar programas que estén dando falsos positivos. ■



AVERIGUA QÚE ES UN ROOTKIT Y DESCUBRE CÓMO DEFENDERTE

SI UN INTRUSO TE CONTROLA...

Los rootkits son programas que se instalan ocultándose en nuestro ordenador y tratan de tomar el control del sistema o extraer información de los discos.

ES UN TIPO DE MALWARE especialista en esconderse de las aplicaciones de seguridad. Se oculta en el disco duro del sistema y, en ocasiones, consigue controlar el ordenador o enviar datos sensibles que éste contenga. Existen distintos tipos de *rootkits*.

Los **persistentes** son los que se activan al iniciar el sistema operativo, ya que se han escondido en el Registro o en el sistema de ficheros para volver a cargarse cada vez que se inicia mediante un código autoejecutable. Algunos llegan a alojarse en el *firmware* de ciertos dispositivos para evitar ser detectados. Otros consiguen incluso cargarse antes que el sistema operativo y cargar el mismo en una máquina virtual. Los segundos son los **rootkits basados en memoria**, que se cargan en la RAM al ejecutar el *malware* que lo contiene, pero no sobreviven a un reinicio a menos que volvamos a ejecutar el mismo programa. Suele asociarse a ejecutables que se supone que vamos a utilizar a menudo. Un tercer tipo son los **rootkits en modo usuario**, sofisticados, que utilizan métodos avanzados para evitar su detección. Por ejemplo, son capaces de detectar si el sistema operativo está realizando un listado del directorio en el que se encuentran, interceptan la ejecución de la API y devuelven un listado en el que no aparecen los ficheros asociados al mismo. Por último, los **rootkit en modo kernel** son capaces de interceptar las APIs, como en el caso anterior, pero también las estructuras de datos del núcleo. Por ejemplo, pueden ocultarse simplemente retirando su presencia de las listas de ejecución del kernel.

Los programas de seguridad suelen tener dificultades para detectar *rootkits*, pues utilizan técnicas para ocultarse que dificultan su funcionamiento. Las aplicaciones que detectan específicamente este tipo de amenazas, comparan los resultados de comprobaciones de diversas variables del sistema utilizando las APIs de Windows con el resultado de realizar las mismas comprobaciones con llamadas de bajo nivel.

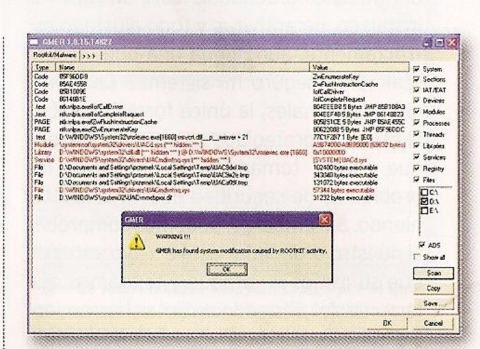
Para la eliminación de estos elementos, existen varias utilidades. También realizan análisis de tipo heurísitco. Los principales fabricantes de software de seguridad diponen de una utilidad para detectar *rootkits*. En **www.antirootkit.com/software**, podemos encontrar una lista con programas que realizan esta tarea. Vamos a mostrar cómo utilizar algunas de estas utilidades.

Maneja los rootkits con Gmer

Es un programa capaz de detectar *rootkits* ocultos de distintos tipos. También es capaz de monitorizar distintas actividades del sistema, como instalación de controladores, carga de librerías, modificación de entradas de Registro y otras actividades potencialmente sospechosas. Podemos descargarlo desde la web **www.gmer.net/files.php**. Curiosamente, y dado que algunos *rootkits* no permiten la ejecución del ejecutable si tiene por nombre **gmer.exe**, la página web crea un archivo ejecutable con un nombre aleatorio.

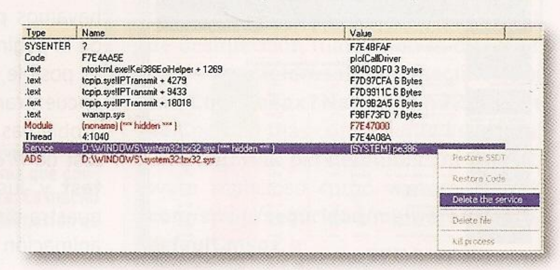
PASO 1 »EJECUCIÓN Y DIAGNÓSTICO

Para detectarlos, ejecutaremos el programa. Veremos en pantalla una ventana en la que haremos clic en el **icono de la doble flecha** de la derecha para desplegar las pestañas. En la ventana **Rootkit/Malware**, elegiremos los procesos y los discos a analizar. Lo recomendable es **marcar todas las opciones si sospechamos que estamos infectados**. Luego, iniciaremos la detección pulsando en **Scan**. Irán apareciendo los resultados del análisis y comparaciones de ficheros de GMER. El software marcará en rojo los procesos, ficheros, servicios o entradas de Registro que sean sospechosas.



PASO 2 »ELIMINA EL ROOTKIT

Para eliminarlo, haremos clic con el botón derecho y escogeremos la opción correspondiente (**borrar o matar el fichero, eliminar el servicio, la entrada del Registro**...). Para más información, copiaremos los datos del fichero infectado y buscaremos en Internet la cadena para saber qué medidas son las que debemos tomar, por si el *rootkit* provocara más problemas. ■



PONEMOS A PRUEBA EL EQUIPO
¿ES SEGURO MI ORDENADOR?

En la Red existen servicios de diagnóstico de seguridad del sistema que permiten detectar problemas en nuestro equipo sin tener que instalar ningún software.

UNA VEZ CONFIGURADA la seguridad de nuestro ordenador, con un *firewall* instalado, un antivirus y todo ajustado correctamente, aún queda una duda: ¿será realmente seguro mi sistema? En condiciones normales, la única forma de saber si estamos protegidos es que las medidas que hemos tomado vayan atajando los problemas de seguridad que vayamos teniendo. Sin embargo, podemos comprobar si nuestro ordenador está a salvo antes de que suframos un ataque y tengamos que lamentarlo utilizando distintas herramientas *on-line*. Vamos a ver cómo funcionan algunas de estas herramientas y cómo pueden ayudarnos a ajustar la seguridad de nuestro sistema.

Hay que tener en cuenta que, para activar algunos de estos servicios, es posible que sea necesario volver a habilitar la ejecución de *scripts* como JavaScript o ActiveX. Para comprobar qué tenemos que volver a activar, consultaremos la documentación del servicio. Cuando termine el análisis, volveremos a desactivar estas funciones.

Comprobación con Test My PC Security

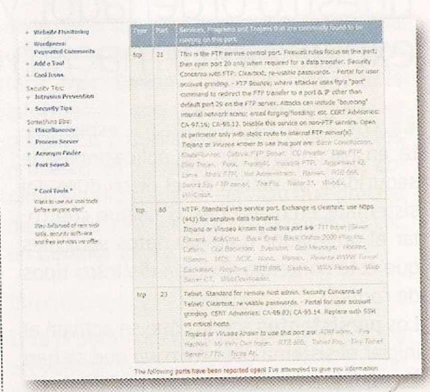
www.testmypcsecurity.com

Se trata de una página web que recoge una larga serie de utilidades que ponen a prueba el funcionamiento de determinadas herramientas de seguridad, como el firewall o el software de seguridad. Así, ofrece la descarga de programas que examinan dos tipos de problemas de seguridad: los referentes al **firewall de tipo firewall leak**, por permitir conexiones salientes sin comprobación; y el **test HIPS**, diseñado para medir la eficacia de la protección del sistema ante cambios del Registro, de archivos críticos del sistema operativo y otros ficheros sensibles. Los programas de prueba son actualizados para ponerse al día con nuevos tipos de ataques. En la página web, accederemos a la pestaña **Download Security test** para descargar uno o todos los programas de prueba de vulnerabilidades. También podemos ver el resultado de los tests de distintas configuraciones realizadas por voluntarios en la pestaña **View Test results**.

Prueba de seguridad con Audit MY PC

www.auditmypc.com

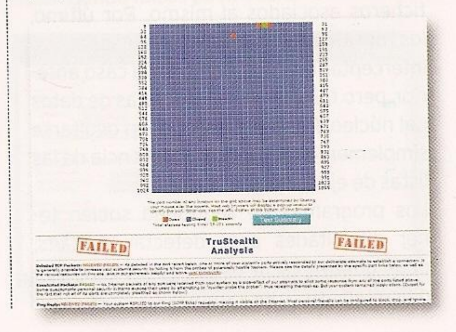
En esta página web, podemos acceder a distintos servicios de **comprobación del sistema** y no solo de seguridad. También es posible realizar **pruebas de velocidad de conexión** y distintos test de nuestro sitio web. Dentro del apartado de seguridad, podemos comprobar la **seguridad** que nos proporciona el **firewall** descubriendo qué puertos tenemos abiertos. También hay una prueba de navegación anónima y un test para constatar si nuestro **navegador** bloquea correctamente la publicidad *pop-up*. En la propia página web, podremos encontrar consejos y programas para solucionar incidentes de seguridad que hayamos podido encontrar con los tests de la página web. En el enlace **HelpDesk**, es posible acceder a un foro en el que se encuentran opiniones de expertos sobre problemas de seguridad. Para ejecutar el test de *firewall*, haremos clic en **Firewall test** y, luego, nos pedirá que copiemos nuestra dirección IP. El test mostrará una animación que indicará que está en marcha. Cuando finalice, veremos una lista de puertos abiertos, si es que ha encontrado alguno en este estado, y los posibles programas *malware* que podrían entrar por dichos puertos.



Test del PC con Shields Up

www.grc.com/x/ne.dll?bh0bkyd2

Al abrir este servicio de comprobación de seguridad, la página web de **Shields Up** mostrará nuestra dirección IP y nombre de máquina con un texto en el que nos permitirá comprobar si la forma de mostrar nuestra dirección revela algún tipo de vulnerabilidad de nuestra conexión. Al pulsar en **Proceed** se pondrá en marcha el diagnóstico de seguridad. Al igual que la prueba de **Audit My PC**, se mostrará un informe de puertos accesible, pero en forma de gráfico. También mostrará el resultado de las pruebas en las que se solicitan paquetes, así como al respuesta al ping.



EVITA ENTRAR EN UNA BOTNET

¿MI EQUIPO ES UN ZOMBIE?

El despliegue de una botnet por parte de un gusano representa una técnica de «reclutamiento» a través de la cual los equipos infectados van formando una red con diversos fines delictivos.

Uno de los peligros más actuales de Internet es que nuestro ordenador sea infectado por *malware* y entre a formar parte de una *botnet*. Cada **ordenador que pasa a formar parte de una de estas redes se denomina zombie**, pues está actuando de forma controlada sin que el usuario lo sepa. Las **botnets** se utilizan por parte de delincuentes informáticos **para** realizar distintas actividades delictivas, como **distribuir** correo **spam**, realizar **ataques de denegación de servicio**, **infectar** la red **con virus** y otras actividades delictivas.

La forma de prevenir que nuestro ordenador sea uno miembro de una *botnet* es tener al día nuestro sistema operativo, tener instalado un software de seguridad y tenerlo actualizado, además de fijarnos en diversos síntomas que pueden revelar que nuestro ordenador ha sido infectado por un gusano para que forme parte de una *botnet*. Una de las razones por la que es difícil detectar la infección de un gusano para crear *zombies* es que estos son discretos.

Las máximas precauciones

Lo primero es tomar las medidas habituales de seguridad. La forma más común de **extender una red de zombies** es **a través de ficheros de redes P2P y programas adjuntos a mensajes de correo electrónico**, por lo que extremaremos las precauciones.

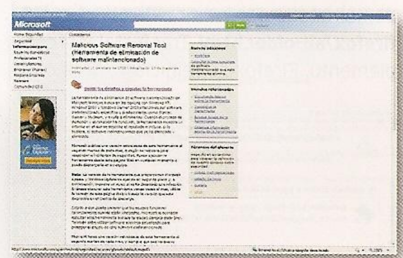
Una forma eficaz de prevenir y detectar el funcionamiento de un gusano para convertir nuestro ordenador en un *botnet* es a través del **firewall**. Si tenemos instalado uno, bloquearemos y monitorizaremos los intentos de conexión saliente desde nuestro ordenador. De esta forma, sabremos que un *malware* está utilizando nuestro ordenador.

Gusanos famosos

Una de las debilidades de las *botnets* es precisamente su extensión. Crean redes tan grandes de ordenadores, en ocasiones, más de un millón de sistemas, que, al final, la infección acaba en todas las páginas web de información de seguridad y normalmente la propia **Microsoft distribuye un parche** para solventar el problema. Es el caso del último y más famoso **gusano** que se ha extendido por Internet, **Conficker**, para el que se detectó su patrón de conducta en todas sus variantes y se pudo desarrollar un parche para la vulnerabilidad del sistema operativo del que se aprovechaba.

Funcionamiento del gusano Conficker

El gusano Conficker, también conocido como **Downadup**, **Downad** y **Kido.ih**, **aprovecha** una **vulnerabilidad en el servicio RPC de Windows** que fue solucionada por Microsoft en octubre de 2008 mediante un parche de seguridad, que, sin embargo, no fue aplicado por un gran número de ordenadores, que, por lo tanto, se hicieron vulnerables al gusano. El ataque tiene lugar enviando una petición inicial al ordenador para comprobar si dispone de protección para la vulnerabilidad. En caso de ser vulnerable, se envía un archivo de *malware* que se instala en el ordenador de la víctima. Entonces, dicho fichero instala en el disco duro del PC un servidor HTTP. Es en ese instante cuando el ordenador empieza a actuar como *zombie* para extender la infección enviando la misma petición que ha recibido inicialmente. Al igual que en el caso anterior, se procede al envío de nuevos archivos infectados en el caso de no tener cerrado el agujero de seguridad.



• La desinfección manual de un sistema que contiene un gusano resulta muy compleja. Es mucho mejor utilizar una herramienta de eliminación de malware para resolver el problema.



• Uno de los vehículos más habituales por el que los gusanos que extienden botnets infectan los ordenadores de los usuarios son las descargas de archivos P2P.

Sin embargo, éste no es el único vehículo que utiliza Conficker para extenderse. Además, este gusano se propaga en redes locales protegidas con **contraseñas débiles** y puede utilizar el **mecanismo de autoarranque de dispositivos USB extraíbles**, como discos duros, *sticks* e incluso cámaras fotográficas. Conficker se registra como un servicio de sistema con nombres aleatorios, por lo que es difícil de localizar. Existe una guía completa de desinfección manual en la dirección web **www.microsoft.com/security/portal/Entry.aspx?Name=Win32/Conficker**, pero lo más conveniente es utilizar un programa para eliminación de software malicioso como **www.microsoft.com/spain/seguridad/malwareremove/default.mspx**. ■

NAVEGA SIN SER DETECTADO

EXPLORACIÓN SIN RASTROS

Algunos navegadores modernos permiten ocultar nuestros datos de navegación mientras los utilizamos, otros precisan de complementos para conseguirlo.

LA NAVEGACIÓN ANÓNIMA es una función cada vez más demandada en Internet. Hay numerosas páginas web y servicios que recogen datos sobre nuestra navegación, detectan nuestra dirección IP e incluso establecen desde qué zona nos estamos conectando. Por otro lado, si nos conectamos por una red pública, también es conveniente no dejar rastros o información sobre nosotros y nuestra actividad en Internet. Los datos que se ocultan son, por un lado, los de la navegación y, por el otro, nuestra propia dirección IP. Como hemos visto, los nuevos navegadores, como **Internet Explorer 8**, **Safari** y **Google Chrome**, disponen de la posibilidad de abrir una ventana del navegador totalmente anónima. **Firefox** tiene previsto incorporar una función parecida en la futura versión 3.1 del navegador. Para otros navegadores, podemos utilizar un complemento de seguridad que oculte nuestra navegación. En este práctico, veremos cómo configurar uno de los más populares complementos para navegación anónima: **Tor**.

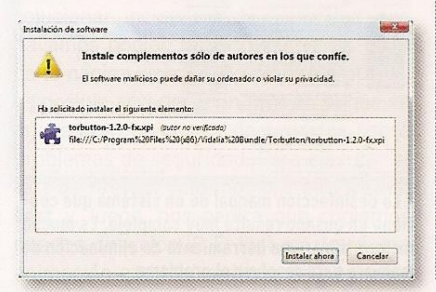
También hay una tercera posibilidad para navegar sin ser controlado y es la de utilizar un navegador especialmente diseñado para ello, como **e-Capsule**. Podemos descargar una versión de prueba de 14 días en **www.eisst.com/products/private_browser**. Este navegador almacena todos los datos de navegación en ficheros encriptados y permite activar la navegación a través de una red de *proxies* para ocultar la dirección IP con la pulsación de un botón. Además, existen utilidades externas para mantener privada nuestra navegación que veremos en los siguientes capítulos.

Instala Tor para Firefox

Tor es un servicio de navegación segura y anónima utilizado por el ejército de los Estados Unidos que se basa en una red de túneles cuyo objetivo es que se pierda el rastro de la conexión de los usuarios que lo utilizan. Es un complemento que solamente protege el transporte de los datos, impidiendo su intercepción. Para ocultar los parámetros de conexión, como la dirección IP, utilizaremos otras herramientas, como *proxies*, o programas específicos, como **Hotspot Shield**. En el paquete completo de utilidades Tor, se incluye un *proxy* privado llamado **Privoxy**. También seguiremos teniendo que cuidar que no se almacenen *cookies* o de ocultar otros datos como el tipo de ordenador. Tor puede instalarse como complemento del navegador Firefox. Vamos a ver cómo instalarlo y cómo se usa. Podemos acceder a la descarga de Tor, además de información sobre el servicio, en su página web **www.torproject.org/docs/tor-doc-windows.html.es**.

PASO 1 »LO INSTALAMOS

En la página de descargas, elegiremos la versión estable para Windows. Al descargar el archivo y ejecutarlo, se iniciará el asistente de instalación. Tras copiar los archivos, el programa instalará el complemento para Firefox correspondiente. Si no lo tenemos cargado, tendremos que hacerlo y volver a ejecutar la instalación. Hay que tener en cuenta que Tor modifica ciertos parámetros, como la zona horaria en Firefox 3. Para descargar Firefox 2, podemos acudir a **www.mozilla.com/en-US/firefox/all-older.html**. Tras instalar el complemento, Firefox se reiniciará. Si el complemento se ha cargado correctamente, veremos en la parte inferior izquierda de la ventana el mensaje **Tor Desactivado**.



PASO 2 »LO ACTIVAMOS

Para conectarnos a la red Tor, comprobaremos que **Vidalia** y **Privoxy** se están ejecutando. Si lo están, aparecerán el **icono de una cebolla** y una **P** rodeada de un círculo azul en la barra de tareas. Si no, los iniciaremos pulsando **Inicio** y escribiendo **Vidalia** y **Privoxy**. Luego, activaremos la red Tor haciendo clic sobre la esquina inferior derecha del navegador. Debería aparecer el mensaje **Tor activado**. Para comprobar



que ya estamos navegando con seguridad, abriremos la dirección **https://check.torproject.org**. Podemos ver un mapa de la red Tor haciendo doble clic en el **icono en forma de cebolla** y eligiendo la opción **Ver la red**. También es posible configurar Tor para otros navegadores, añadiendo en las opciones como *proxy* el activado por **Privoxy** en la dirección **localhost** y el **puerto 8118**. También puede configurarse para mensajería instantánea y otros programas a través de **SOCKS** en la dirección **localhost**, **puerto 9050**. Si tenemos instalado un *firewall*, hay que agregar permisos para acceder a los puertos **8118** y **9050** en conexiones entrantes y los puertos **TCP 80** y **443** en conexiones salientes. ■

NO EXPONGAS TUS MENSAJES
PON A SALVO TODO EL CORREO

Además de la navegación web, también nuestros mensajes de correo pueden encontrarse en una situación de riesgo, a no ser que los protejamos con herramientas como PGP.

EL CORREO ELECTRÓNICO es otro de los servicios más utilizados en Internet y, al igual que la navegación, también tiene sus problemas de seguridad. Las comunicaciones pueden ser interceptadas tanto «cazando» correos electrónicos en la red como con ataques de *hackers* que accedan a los servidores de correo. Para evitar que alguien pueda leer nuestro correo electrónico privado, utilizaremos **herramientas con técnicas criptográficas**. Ya hemos visto cómo la criptografía puede ayudar a proteger nuestro disco duro y las unidades de almacenamiento cifrando su contenido para que solo el propietario pueda descifrarlo. En este caso, utilizaremos el programa **PGP Desktop**, que instalamos para realizar la codificación del disco duro.

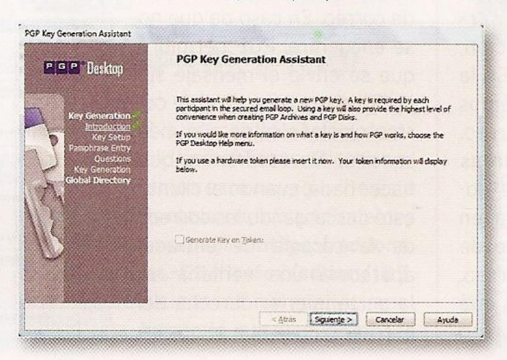
El sistema de protección de contenido PGP permite codificar mensajes y documentos de forma que solo alguien autorizado o el destinatario de estos documentos pueda verlos gracias a un sistema de claves de alta seguridad. El programa utiliza el **sistema de clave pública**, por lo que intercambiaremos mensajes cifrados con todo aquel que se haya incorporado a la base de datos de claves de PGP. Es decir, cualquiera que quiera enviarnos un mensaje utilizará nuestra clave pública para hacerlo. Cuando lo recibamos, nuestra **clave privada** nos permitirá leerlo. La clave pública sólo sirve para cifrar mensajes, no para descifrarlos. De esta forma, únicamente el que posea la clave privada asociada a la clave pública que escojamos para codificar el mensaje podrá leerlo. Existe una base de datos de claves públicas de PGP que es la que utilizaremos para crear nuestro mensaje. Hay que tener en cuenta que la persona que lo reciba también tendrá que tener instalado el programa. A continuación, vamos a ver cómo cifrar un *e-mail* o sus documentos adjuntos. La dirección de descarga es **www.pgp.com/downloads/desktoptrial/desktoptrial2.html**.

PASO 1 »CREA LA CLAVE

El primer paso será crear tanto la clave pública como privada y publicarla para que cualquiera que quiera enviarnos un mensaje confidencial pueda hacerlo buscando nuestro nombre en la base de datos. Haremos clic en el menú **File/New PGP Key**. Luego, seguiremos los pasos que nos va proponiendo el asistente para crear nuestra clave, tal y como hicimos para codificar el disco en el apartado correspondiente. En cambio, esta vez no saltaremos el último paso, que nos permitirá acceder al directorio global de PGP para grabar nuestra clave pública. Si ya hemos creado una clave, como la que hemos necesitado para codificar el disco duro, simplemente seleccionaremos la nuestra y abriremos el menú **Key/Publish to global directory**.

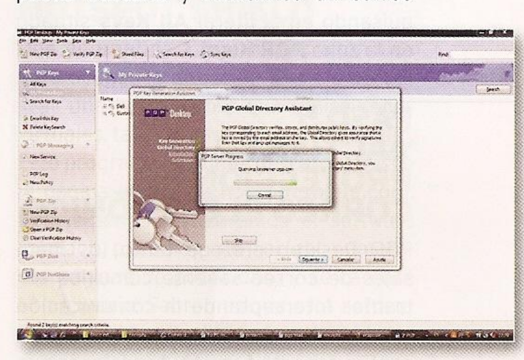
PASO 2 »EXPORTA LA CLAVE PÚBLICA

Cuando tengamos en pantalla el asistente **PGP global directory assistant**, pulsaremos en **Siguiente**. El programa conectará, en primer lugar, con la base de datos de claves públicas de PGP para sincronizar los datos con nuestro programa. La siguiente acción será guardar una copia de nuestra clave para que podamos utilizarla en otros ordenadores o, simplemente, como medida de seguridad. Hay que tener presente que, para que sea útil, tendremos que recordar la contraseña (**passphrase**) que hemos utilizado para crearla. Sin esa palabra, ni siquiera podremos borrarla. Para realizar una copia, pincharemos sobre nuestra clave y luego en **File/Export/Key**. Elegiremos un lugar donde almacenar la clave. Para recuperarla, haremos lo mismo, pero, en el menú **File**, escogeremos **Import**.



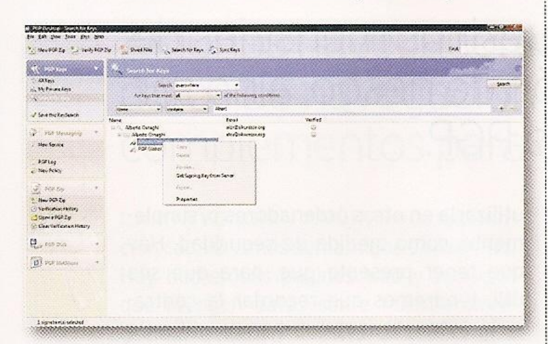
PASO 3 »COMPARTE CLAVES

Además de enviar nuestra clave al directorio de claves para que cualquier usuario pueda buscarla y remitirnos un correo electrónico cifrado, puede ser útil mandarla directamente a nuestros contactos para que la tengan a su disposición siempre que quieran enviarnos algún mensaje. Para hacerlo por correo, haremos clic con el botón derecho en la clave y elegiremos la opción **Send to/Mail recipient**. Se iniciará un asistente que nos pedirá el nombre para identificar el mensaje que contendrá la clave. También tendremos que dar los datos de nuestro servidor de correo electrónico para enviar el *e-mail* correctamente. ▶



PASO 4 »CODIFICA EL E-MAIL

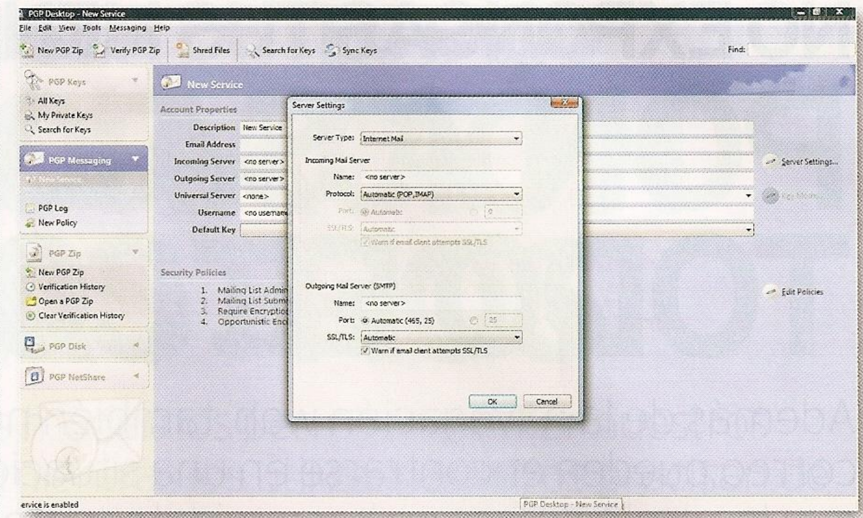
Para codificar el mensaje correctamente, necesitaremos tener la clave del destinatario, de manera que solo pueda leerlo el usuario que va a recibirlo. Como hemos visto unas líneas atrás, nos la pueden enviar por correo electrónico si no se quiere compartir la clave con otras personas, pero también podemos buscarla en el directorio de claves de PGP. Si nos decantamos por esta última alternativa, nos dirigiremos



a **PGP keys/Search for keys**, con lo que aparecerá un buscador a través del cual comprobaremos si nuestro contacto tiene clave pública almacenada en el servidor. Para ello, introduciremos el nombre en la casilla de búsqueda y pulsaremos en la tecla **Enter**. Una vez localizado, haremos clic con el botón derecho del ratón sobre su clave y elegiremos **Get signing key from server**. Luego, en la ventana que se lanza, seleccionaremos las claves y pincharemos en **Import**. Por último, comprobaremos si la clave se muestra en nuestra lista de claves pulsando en el literal **All Keys** situado en la zona **PGP Keys**.

PASO 5 »ACTIVA LA PROTECCIÓN DE CORREO ELECTRÓNICO

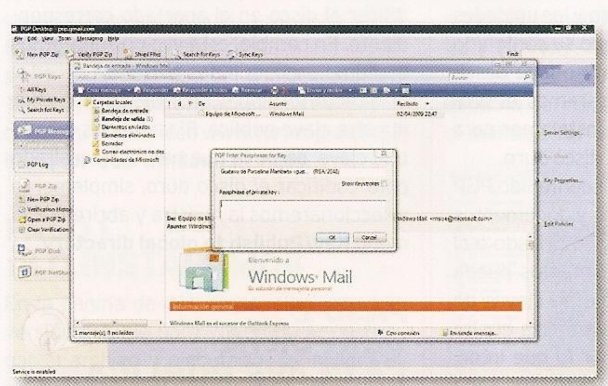
PGP Desktop protege tanto los mensajes de correo saliente como los entrantes interceptando la comunicación con nuestro servidor de correo. Para configurar esta función, tendremos que introducir los parámetros de nuestro servicio de correo electrónico. Así, acudiremos a **PGP Messaging/New service**. Para seguir con la configuración, haremos clic en **Server Settings**. En la ventana que aparece, introduciremos los datos de nuestro servidor de correo. Luego, pincharemos en **Email Address** e introduciremos la dirección de correo electrónico. De la misma forma, en **Username**, anotaremos el nombre de usuario de nuestra cuenta de correo. Luego, en **Default key**, elegiremos qué clave asociamos a esta cuenta de correo



electrónico. También podemos intentar que PGP detecte automáticamente la cuenta abriendo el cliente y enviando un mensaje o activando la recepción de mensajes.

PASO 6 »ENVÍO DE CORREO CIFRADO

Para enviar un mensaje de correo electrónico cifrado, abriremos nuestro cliente de correo y lo redactaremos. En el asunto del mismo, escribiremos **[PGP]**. Al enviarlo,



PGP Desktop interceptará el proceso y comprobará la dirección del destinatario. En primer lugar, comparará la dirección de correo electrónico de destino con las claves que tenemos guardadas en local. Luego, buscará en el archivo de claves públicas de PGP para ver si existe clave pública para esa dirección de correo. En caso de que no se encuentre, PGP permitirá que se envíe el mensaje sin codificar. La recepción de correo electrónico es aún más sencilla. No tendremos que hacer nada, cuando el cliente esté descargando los correos de la carpeta de entrada, aparecerá una ventana en la parte inferior derecha del escritorio en la que se nos irá informando del progreso de descarga y en su caso descodificación de mensajes.

PASO 7 »ESTABLECE CIERTAS POLÍTICAS DE FUNCIONAMIENTO

Podemos definir qué comportamiento tiene la encriptación de correo electrónico en ciertas situaciones creando políticas de funcionamiento. Con este propósito, haremos clic en la cuenta de correo y, en la ventana de configuración, pulsaremos en **Edit Policies**. Podemos crear estas políticas dependiendo de condiciones como el contenido del campo **Asunto** o la prioridad y otros parámetros del mensaje. Las acciones que se pueden llevar a cabo son las de **firmar el mensaje**, **codificarlo** o **no hacer nada**. También tenemos la posibilidad de generar una lista de direcciones y establecer acciones determinadas dependiendo de la dirección del remitente o del destinatario del mensaje. Es posible editar las políticas haciendo clic en **Edit policy** y crear otras nuevas con **New policy**. ■

UN ORDENADOR ILOCALIZABLE
ESCONDE TU DIRECCIÓN IP

Cuando nos conectamos con un PC portátil a una red pública o al abrir ciertas páginas web, corremos el peligro de que se utilice nuestra dirección IP para atacarnos

LA DIRECCIÓN IP permite que los paquetes de datos lleguen a nuestro ordenador. Ésta se suele asignar de forma dinámica por nuestro proveedor de Internet, como hemos visto en otro capítulo. En realidad, es el *router* el que recibe una dirección IP y éste se encarga de que los datos lleguen a nuestro ordenador. Proteger nuestra dirección IP puede ser muy importante en distintas situaciones.

En primer lugar, al conectarnos a una red pública WiFi, aunque sea de pago, el que se pueda detectar nuestra dirección IP puede permitir a otras personas acceder a nuestro ordenador. Ocultar nuestra dirección IP también no protege de ciertos tipos de ataques al navegar por determinadas páginas web. Otra gran ventaja de encubrir la dirección IP de nuestro ordenador es la de poder utilizar servicios que estén restringidos para usuarios de ciertos lugares del mundo. En Estados Unidos, existen múltiples servicios con este tipo de restricciones. Para esconder nuestra IP, podemos utilizar varios métodos. El primero es utilizar un **proxy anónimo**. Un *proxy* es un servidor que sirve de intermediario entre el que realiza las peticiones y el servidor. De esta forma, la dirección IP que se muestra a la Red es la del *proxy* y no la del ordenador que está realizando las peticiones.

Utiliza proxies anónimos

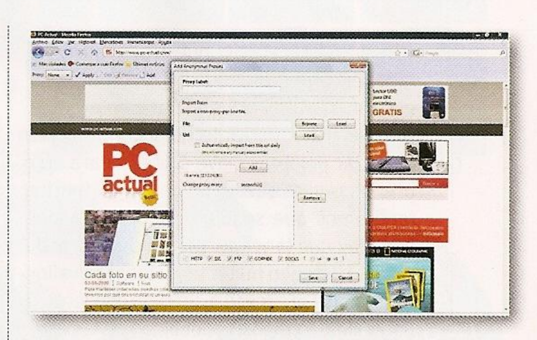
Existen distintas posibilidades para utilizar un *proxy* anónimo. La más directa es acceder a las páginas web de algunos de servicios como **www.proxify.com**, **www.anonymouse.org** o **www.the-cloak.com**. En ellos, simplemente escribiremos la dirección web que queremos visitar en la casilla correspondiente que aparece en el servicio y navegaremos de forma anónima. Algunos permiten configurar ciertos parámetros como la **conexión segura por HTTPS**. En ciertos casos, son versiones gratuitas con limitaciones, por ejemplo, de ancho de banda. Hay que tener en cuenta que los servicios tienen que ser de confianza, pues ellos sí pueden guardar los datos de nuestra conexión. Es conveniente leer las condiciones del servicio para ver qué tipo de protección de la privacidad nos proporciona. También hay otras dos formas de utilizar estos *proxies*: a través de la configuración del navegador o con un complemento especial.

PASO 1 »AJUSTA EL PROXY EN EL NAVEGADOR

En primer lugar, buscaremos las direcciones IP de *proxies* anónimos de confianza. Existen listas *on-line* en direcciones como **www.samair.ru/proxy** o **www.multiproxy.org/anon_proxy.htm**. Luego, accederemos a la configuración de Internet. Haremos clic en **Inicio/ Panel de Control/ Redes e Internet/Opciones de Internet**. Enseguida, abriremos la pestaña **Conexiones/Configuración LAN**. En la ventana que aparece, pincharemos en **Usar servidor proxy**. Aquí será donde introduciremos la dirección IP que hemos conseguido antes. Pulsaremos en **Avanzadas** si se trata de distintos *proxies* para diferentes aplicaciones de Internet.

PASO 2 »INSTALA SWITCHPROXY TOOL

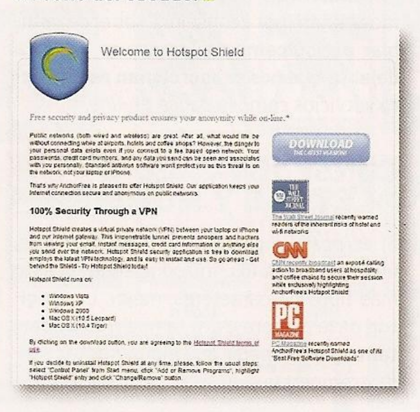
Se trata de un complemento para Firefox que cambia la configuración de la conexión periódicamente modificando el *proxy* que usamos para navegar. De esta forma, se aumenta la seguridad. Podemos descargarlo en la página **https://addons.mozilla.org/es-ES/firefox/addon/125**. Una vez reiniciado el navegador, aparecerá una barra de herramientas que



nos indicará qué *proxy* está utilizando el complemento para proteger la conexión. Para agregar los *proxies* que vamos a utilizar, acudiremos al botón **Add**.

PASO 3 »UTILIZA HOTSPOT SHIELD

Una alternativa a los *proxies* anónimos para ocultar la dirección IP es la de utilizar una herramienta que utilice redes virtuales, tal es el caso de Hotspot Shield. Este programa se puede descargar desde la página web **www.hotspotshield.com**. Simplemente, instalaremos el software (cuidado, pues hay que sortear numerosas páginas de publicidad) y se cargará en memoria. Sabremos que está actuando cuando veamos en la barra de tareas el **icono del escudo**. ■



GENERA CONTRASEÑAS FUERTES

ELIGE BIEN QUÉ CLAVE USARÁS

Uno de los habituales flancos débiles en cuanto a la seguridad de nuestro ordenador y nuestros datos son las palabras clave o passwords de baja calidad y, por tanto, fáciles de adivinar.

PARA AUMENTAR nuestra seguridad, también tenemos que utilizar el ingenio e idear palabras clave lo suficientemente seguras. Es importante no ser previsibles o utilizar palabras clave cortas... Para que una *password* sea definida como fuerte, tendremos que seguir ciertas precauciones. Hay que tener en cuenta que normalmente protegen nuestros datos más valiosos, incluso el acceso a cuentas corrientes. Según los expertos, la debilidad de las contraseñas es uno de los problemas de más habituales tanto en entornos empresariales como domésticos.

Vamos a ver una serie de consejos que nos ayudarán a generar palabras clave más



robustas. Antes de empezar, el que podríamos denominar «consejo 0» es el de **cambiar periódicamente las claves y nunca dejar la que nos proporcionan por defecto** servicios como la banca *on-line*.

CONSEJO 1
»LETRAS Y NÚMEROS

Si es posible, **combina letras, números, incluso símbolos** introduciendo cuanto más tipos de caracteres, mejor. La **longitud** de la palabra clave también **es importante** para impedir que algún *hacker* pueda «romperla».

CONSEJO 2
»PARA RECORDARLAS

Un posible inconveniente a la hora de introducir símbolos y números en la clave es que ésta será más compleja de recordar. Para procurar no olvidarla, podemos sustituir combinaciones de letras por símbolos y números que las representen. Una técnica clásica es la de sustituir la letra **o** por el número **0** o la anotación de **tres letras** por el número **3**. En lo que respecta a los símbolos, por ejemplo, sustituir **menos** por **-** y **más** por **+**.

CONSEJO 3
»OTROS RECURSOS

Otra posible **regla nemotécnica** que nos puede facilitar mucho la tarea de recordar una clave larga y compleja es la de utilizar frases con **palabras complejas** y **que nos sugieran algo a nosotros**, algo realmente personal que sea difícil de adivinar. Podemos convertir la frase en una clave intercalando símbolos (como guiones) y números.

CONSEJO 4
»DESCARTA LO LÓGICO

Evita secuencias lógicas de caracteres y **números y teclas que se encuentren cerca en el teclado**, ya que los programas que descifran las claves suelen utilizar este tipo de estrategia para dar con ellas.

CONSEJO 5
»EL USUARIO DISTINTO A LA CLAVE

Nunca has de introducir el nombre de usuario en la clave. **Tampoco hay que utilizar nuestro nombre o datos personales**, incluso nombres de mascotas o de parientes y amigos. Con la proliferación de blogs y redes sociales esos datos no son ya tan privados. Los algoritmos para romper claves también utilizan el nombre de usuario para debilitar la clave y restringir el número de combinaciones.

CONSEJO 6
»MANTÉN VARIAS

Jamás emplees la misma password para distintos servicios. Eso debilita la seguridad y nos exponemos a que el daño se multiplique.

CONSEJO 7
»MODIFÍCALAS

Si queremos recordar todas nuestras *passwords* y todas ellas son distintas, podemos **crearlas siguiendo la misma regla, pero modificándolas según el nombre del servicio** al que accedemos.

CONSEJO 8
»NO LAS APUNTES

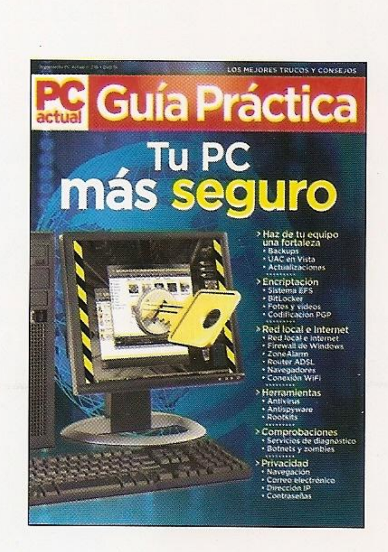
Evita siempre que puedas anotar la palabra clave en papeles o post-it.

CONSEJO 9
»GENERADORES

En caso de que se te acabe la imaginación, es posible usar un generador automático de palabras clave, pero serán prácticamente imposibles de recordar, aunque muy seguras. Podemos encontrar uno en **www.grc.com/passwords.htm**.

CONSEJO 10
»PRUÉBALA

Cuando tengamos la contraseña que creamos perfecta, es hora de ponerla a prueba. Para ello, acudiremos al servicio **Password Meter** (**www.passwordmeter.com**, que además nos dará más pistas de cómo mejorarlas. ■





López de Hoyos, 141, 1º. 28002 Madrid (España)
Tel. 91 510 66 00. Fax 91 519 48 13